Office of Information and Technology
Product Development

Home Telehealth Reporting Enhancements (HTRE)
Integrated Home Telehealth Application (IHTA)

Production Operations Manual

August 2015

Document Version 2.4

Revision History

Date	Version	Description	Author
08/17/2014	2.4		
01/9/2015	2.3	Updates according to Operations Team review January 2015, which include updates to team members contact information, edits to backup testing and network sections, replaced Architectural and Application Components diagrams, and removed Appendices A and B.	Danielle Haile
04/10/2014	2.2	Updates according to Operations Team review March 2014 review (Rashaka Boykin); added Census Activity Reports to permissions table	Katie Shepherd
02/24/2014	2.1	Added the permission/functionality, “Generate Patient Survey Reports” to Tables 5 & 6; reviewed Primary/Secondary Contact Information and updated date	Katie Shepherd
12/6/2013	2.0	Labeled the permission in Table 5, IHTA Permissions (Search Inventory by Patient) as removed from the database (per CCR1094); removed the Search Inventory by Patient functionality from the following roles in Table 6, IHTA Roles: Care Coordinator, National Administrator, VISN/Facility Administrator, and Program Support Assistant.	Katie Shepherd
10/31/2013	1.9	Updated to new ProPath template version 1.1 (March 2013)	Noel Morrison / Chris Woodyard / Katie Shepherd
07/08/2013	1.8	Added specific functionality to the HT Reports module; changed the “NAC POC” role to “OTS Contract Manager”; added the updated Switchover Instructions (per Noel Morrison); added the updated Installation Instructions to Appendix D (per e-mail from Noel Morrison on 7/8)	Katie Shepherd
04/12/2013	1.7	Updated Table 2 to include the new Dell PowerEdge servers at Martinsburg/Hines; updated Figure 2 to include “HT Reports” and the “HDR”; added a brief HT Reports module description to the first paragraph in Section 2; updated the production software in Table 3; added the updated Build Instructions (from Maureen Hafner) to Appendix E; added the HT Reports functionality to the Management role in Table 6 changed references to the Sunshine Telehealth Training Center to the Home Telehealth National Training Center; removed reference to CISS servers in Section 2.3 (In release 5.5, IHTA operates on own servers).	Katie Shepherd
01/15/2013	1.6	Updated the DMP permission in Table 6 to include Add & View Comment functionality and assigned DMP Reviewer role; changed Falling Waters to Martinsburg for production environment.	Katie Shepherd
08/10/2012	1.5	Updates to the DMP permission in Table 6; added the use of the National Service Desk and Remedy to Section 7	Katie Shepherd
03/06/2012	1.4	Added Section 7.2.1 (support procedures for Inventory Tracker) and 7.2.2 (support procedures for the DMP module); added the DMP permissions IDs to Table 6.	Katie Shepherd
01/17/2012	1.3	Updated Table 5 to include all permissions assigned to each role; also added the System Administrator role. Updated Table 6 with a note stating that the marked permissions were removed from database in January 2012.	Katie Shepherd

Date	Version	Description	Author
11/03/2011	1.2	Updated Installation Instructions (Appendix D) to include the reference of the deployment of .dmp.zip On-Line file to all environments; added text to Section 2 describing the DMP module; added Sections 3.4.1 and 3.4.2.	Katie Shepherd
08/31/2011	1.1	Changed project name to Home Telehealth Capability Enhancements (HTRE); updated for Release HTRE 3.5; added the IHTA Installation Instructions as Appendix A and the CCHT-IHTA Build Instructions as Appendix D; updated Section 3.4 to include who is responsible for system monitoring; removed Template Version from the title page.	Katie Shepherd
03/31/2011	1.0	Baseline release	Vu Le

Table of Contents

1 Introduction

The Integrated Home Telehealth Application (IHTA) is a Web-based system, providing a flexible, maintainable, and resilient platform for Home Telehealth (HT) business functions. IHTA facilitates the retrieval of home device information for tracking device inventory, managing Quality Improvement Reports (QIR), and generating reports on device availability and vendor compliance. IHTA is also used for the development, storage, and retrieval of Veteran Health Administration (VHA) Disease Management Protocols (DMP). Finally, the HT Reports module of IHTA allows users to review and search HT data via various management report options. There are 23 Veteran Integrated Service Networks (VISN), providing centralized information technology (IT) support to 168 medical centers. IHTA will be used by all VISNs, to ensure a standard way of managing device information and QIRs at all VA facilities.

IHTA comprises two fully operational, load balanced systems, one at the Primary Facility and the other at the alternate location at the Secondary Facility. The Primary and Secondary facilities will alternate between the Martinsburg Capitol Region Readiness Center (CRRC) (Martinsburg, WV) and the Hines Information Technology Center (HITC) (Hines, IL). Each site will have equal capacity and will be capable of supporting users as the operational site. IHTA will be accessible from the various VISNs, each accessing the central IHTA and HT databases, facilitating the management of device information.

The IHTA database architecture is configured for complete redundancy. During operational hours, the data is replicated from the Primary to the Secondary Facility, at near real-time. This process ensures that in the event of a catastrophic failure, if the production database cannot be restored, there will be minimal loss of data, and the alternate database can replace the production database.

IHTA uses database servers which are fully redundant between the Primary and Secondary Facilities. In the event that the database at the Primary Facility goes down, the system will shift operations to the redundant database at the Secondary Facility, via the database mirroring component of Microsoft SQL Server. The switch to the redundant database will require manual intervention, but will be transparent to the users.

The databases will be replicated asynchronously from the Primary to the Secondary Facility site with a maximum transaction replication lag time of 15 minutes. Switching between the two sites and operating from each site is essential to ensure that there is minimal downtime and that the latest data is available to the users. A user who is signed in at the time of the switch to the alternate site will be interrupted, and there may be a minimum data loss.

Only authorized users will be able to access IHTA. Role-based access control is set up and maintained by an administrator at the National/VISN/Facility level ensuring users have access to the appropriate level of information.

1.1 Operational Priority and Service Level

Support will be performed by the National Service Desk – Tuscaloosa (NSD) (Tier 1 Support), Product Development (PD) Product Support Team (Tier 2 Support), and the IHTA Support Group (Tier 3 Support).

The IHTA Support Team utilizes the following VA distribution list:
VAOITOEDIHTASupport@va.gov

The following team members are included in this list: Rashaka Boykins (Operations), David Komraus (Project Manager), Kristen Kriwox (Business Analyst), Bill May (Developer), Chuck Lee (System Administrator), Chris Woodyard (DBA), and Kate Hula (Technical Writer).

Tier 1 Support will be provided by the NSD utilizing the Remedy system. IHTA users with problems that cannot be resolved locally will call the NSD to open a Remedy ticket. Issues not resolved by the Tier 1 Support Team will be assigned to Tier 2 Support in Remedy. Tier 2 Support for IHTA will include assistance from the PD Product Support Team. Issues not resolved by the Tier 2 Support Team will be assigned to Tier 3 Support in Remedy. Tier 3 Support is the highest level of support for IHTA, which includes business analysts, software testers, system administrators, developers, and database administrators who have specialized technical knowledge of IHTA. Tier 3 Support will provide services, such as, issue resolution and defect management on all issues/defects that have not been resolved by the Tier 1 and 2 Support Teams. Any defect found will be logged in Remedy and also in Rational ClearQuest (as required).

Table 1 outlines the incident priority levels and the time frame for response:

Table 1: IHTA Incident Priority Levels and Time Frame for Response

Priority Level	Call Received	Time Frame for Response	Priority Level Description
Urgent	During business hours	Requester will be directly contacted by Service Provider	An urgent incident is a catastrophic incident of an operating environment where production systems are severely impacted, down or not functioning. Under this scenario, one of the following situations may exist: • Loss of production data and no procedural work around exists. • Patient care and/or safety are at risk or damage is incurred. • Complete loss of a core organizational or business process where work cannot reasonably continue.
	During non-business hours		
High	During business hours	Requester will be directly contacted by Service Provider	A high incident is a problem where a system is functioning but in a severely reduced capacity. The situation is causing: • Significant impact to portions of the business operations and productivity. • No loss of production data and / or a procedural work around exists. • The system is exposed to potential loss or interruption of service. Includes incidents that significantly impact development and/or production, but where an alternative operation is available.
	During non-business hours		
Medium	During business hours	Average of two (2) business hours or less	A medium incident is a medium-to-low impact problem which involves partial non-critical

Priority Level	Call Received	Time Frame for Response	Priority Level Description
	During non-business hours	No After Hours Coverage will be provided	functionality loss. A medium incident impairs some operations but allows the user or an application to continue to function. This may be a minor incident with limited loss or no loss of functionality or impact to the user's operation and incidents in which there is an easy circumvention or avoidance by the end user.
Low	During business hours	Average of eight (8) business hours or less	A low incident has no impact on the quality, performance, or functionality of the system. Low incidents have minimal organizational or business impact.
	During non-business hours	No After Hours Coverage will be provided	

Also refer to the Service Level Agreement (SLA) for Information Technology Services between the Veterans Health Administration Care Coordination Services/Care Coordination Home Telehealth organization and OI&T located on the HTRE TSPR at the following link: http://tspr.vista.med.va.gov/warboard/ProjectDocs/Home_Telehealth_Development/HT_SLA_Draft_March2013.pdf

1.2 Logical System Description

Application layering generalizes the various functional layers in the architecture (see Figure 1). For IHTA, its HTML-rendered content implements the standard Struts2 Web framework, injected with Spring components called business services. IHTA uses the Flex library to render its content and HTTP requests are tunneled through a servlet (BlazeDS) connected to a Spring controller. The Spring controller will then interact with a Spring business service, rules engine, workflow engine, and JPA persistent component.

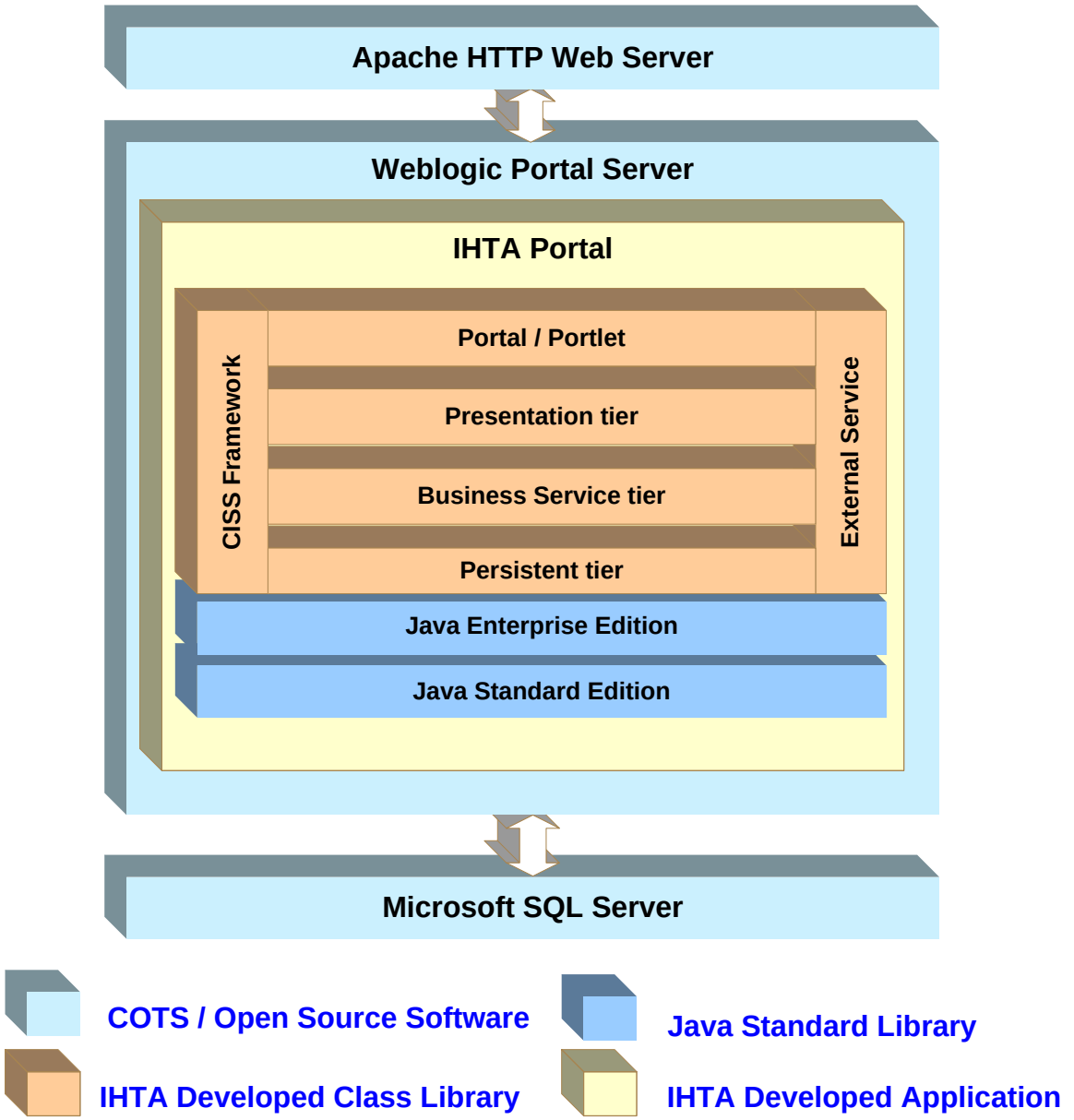

Figure 1: IHTA Architectural Layers

1.2.1 Technology Stack

Figure 2 identifies and groups core IHTA technologies.

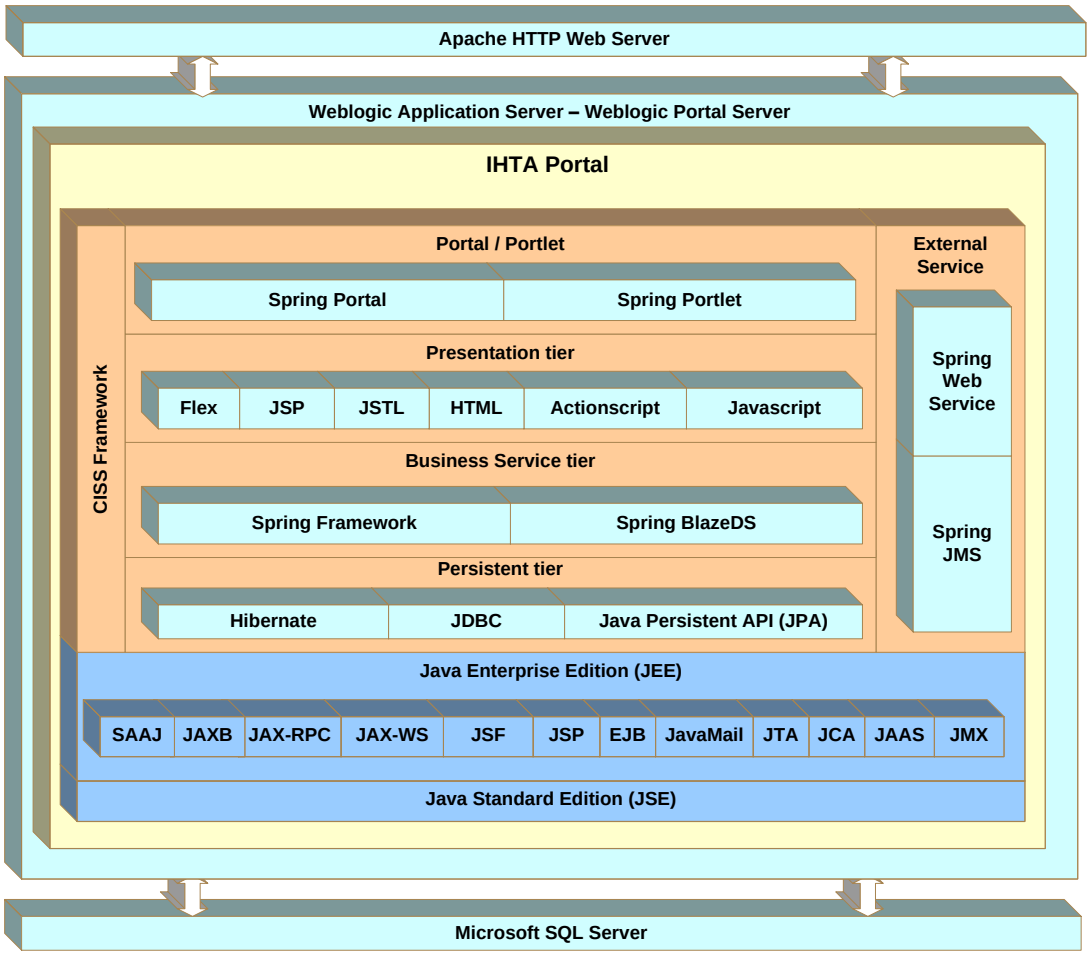

Figure 2: IHTA Technology Stack

1.2.2 Application Components

IHTA modules represent a logical grouping of Java classes and components that are implemented to perform the same or similar business functions. IHTA module codebase uses the IHTA common codebase to ensure a consistent User Interface (UI), well-defined business entities through domain classes, and centralized business logic defined in business services. The following figure depicts IHTA modules and components.

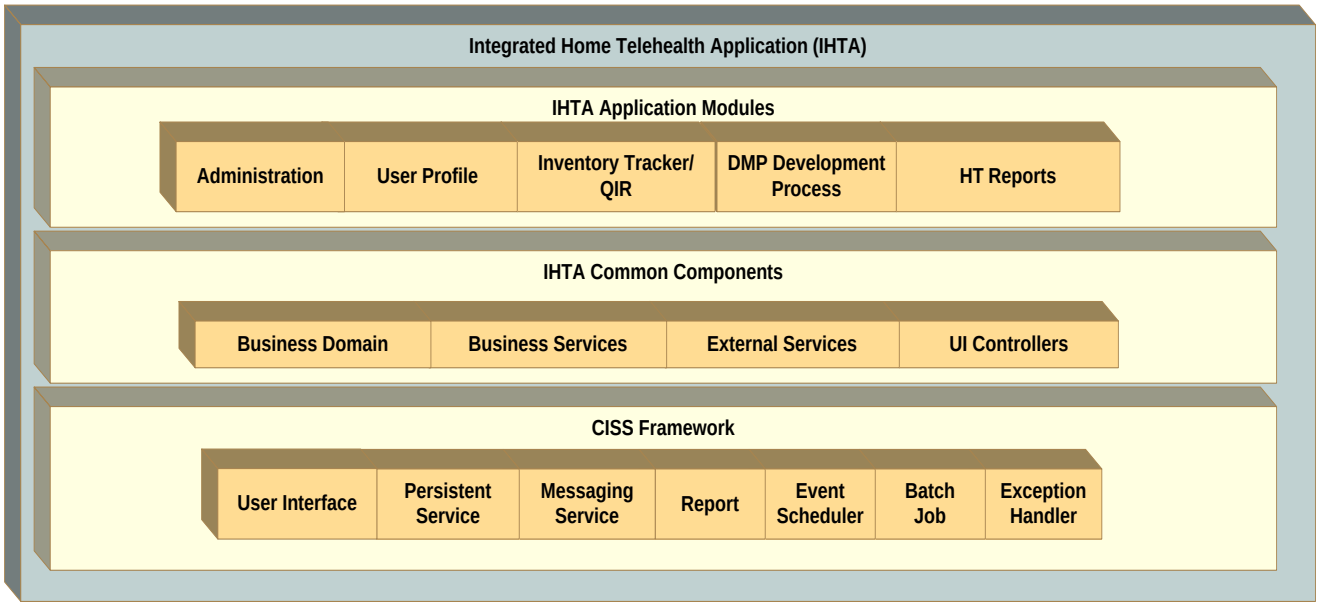

Figure 3: IHTA Application Components

1.3 Physical System Description

Figure 4 provides a high-level overview of the IHTA production environment.

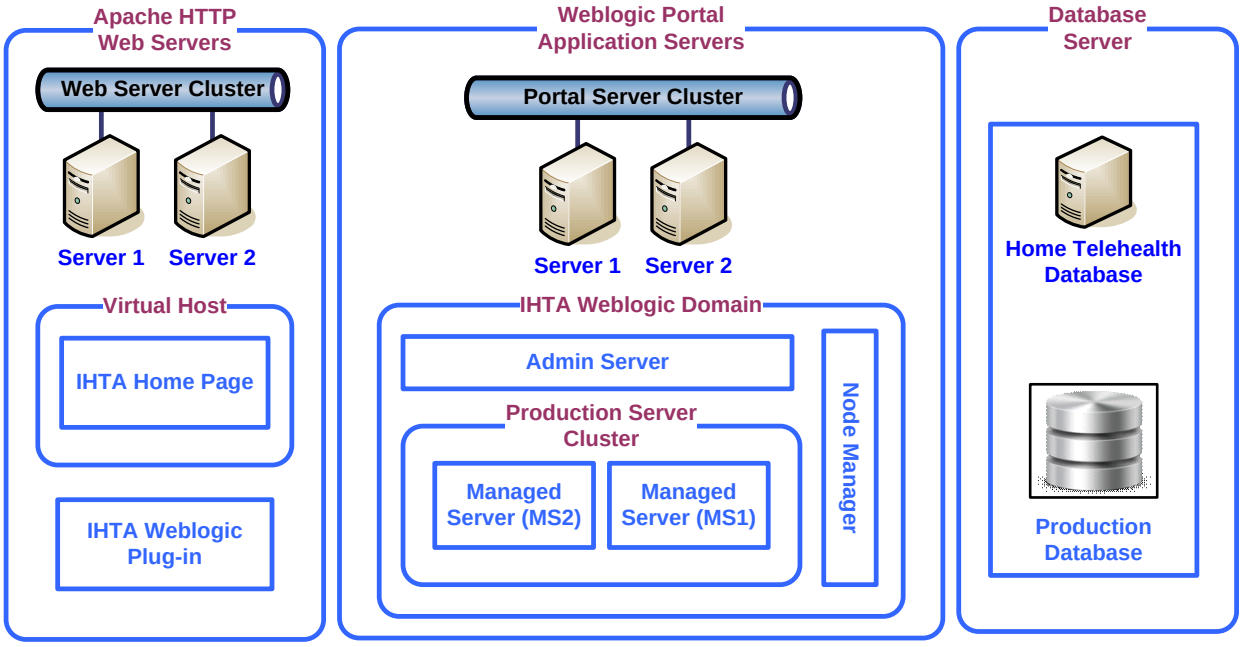

Figure 4: Environment Overview

The computer hardware for the production servers at both Martinsburg and Hines are listed in Table 2. The IHTA SA, Chuck Lee, tracks the warranty status and depreciation cycle using the following Dell Website:
http://www.dell.com/support/home/us/en/19/Products/?IsTag=True&Selection=9KT6VQ1&ProductCode=poweredge-r510&ProductName=PowerEdge%2520R510

The expiration date on all servers below is 6/21/14. A separate spreadsheet is also maintained on the HTRE SharePoint site.

Note these facilities alternate as the Primary and Secondary IHTA production sites.

Table 2: IHTA Server Hardware

Manufacturer	Model, Description, Serial Number	Qty	Warranty Expiration Date
Martinsburg			
Dell	PowerEdge R510 • Application Servers: Serial Numbers: HFS6VQ1, 1GS6VQ1 • Web Servers: Serial Numbers: 8KT6VQ1, FKT6VQ1	4	06/21/2014
Hines			
Dell	PowerEdge R510 • Application Servers: Serial Numbers: CKT6VQ1,DKT6VQ1 • Web Servers: Serial Numbers: BKT6VQ1,9KT6VQ1	4	06/21/2014

1.4 Software Description

Table 3 lists the current software for the IHTA production environment. Note that the following Hardening server guidelines were for followed for Linux:


Red Hat Linux - Baseline Configuratio

Table 3: IHTA Production Software

Required Software	Version	Manufacturer
Microsoft SQL Server	2008	Microsoft
Oracle WebLogic Server	11*g* Release 1 (10.3.5)	Oracle
Apache HTTP Server	Version 2.2.3	Apache
Red Hat Enterprise Linux (RHEL)	5.10	Red Hat

1.4.1 Background Processes

The background processes utilized in IHTA are described in the following subsections.

1.4.2 Job Schedules

Quartz Scheduler is used to manage the scheduled job feature of IHTA. This feature allows administrators to set up and automatically execute various pre-defined scheduled jobs. IHTA currently executes the following scheduled jobs at periodic intervals**:**

- Purge Completed Reports: Deletes all reports in the application that have expired.
- Weekly Vendor Compliance Report: Allows users to schedule the automatic e-mail of Inventory Tracker's *Weekly Vendor Compliance Report*.
- QIR Vendor Response Due: Generates a notification to the Vendor when the *Vendor Response Due Date* has passed in the QIR functionality of Inventory Tracker.

Java Messaging Services (JMS) is utilized for internal communication between IHTA components to invoke asynchronous tasks, including, but not limited to, user registration, the vendor response due notice, and to schedule reports. The JMS Subscriber distributes e-mails for notification.

1.4.3 Dependent Systems

Figure 5 illustrates the enterprise systems that IHTA interfaces with. The details of the enterprise services and applications are summarized in Table 4.

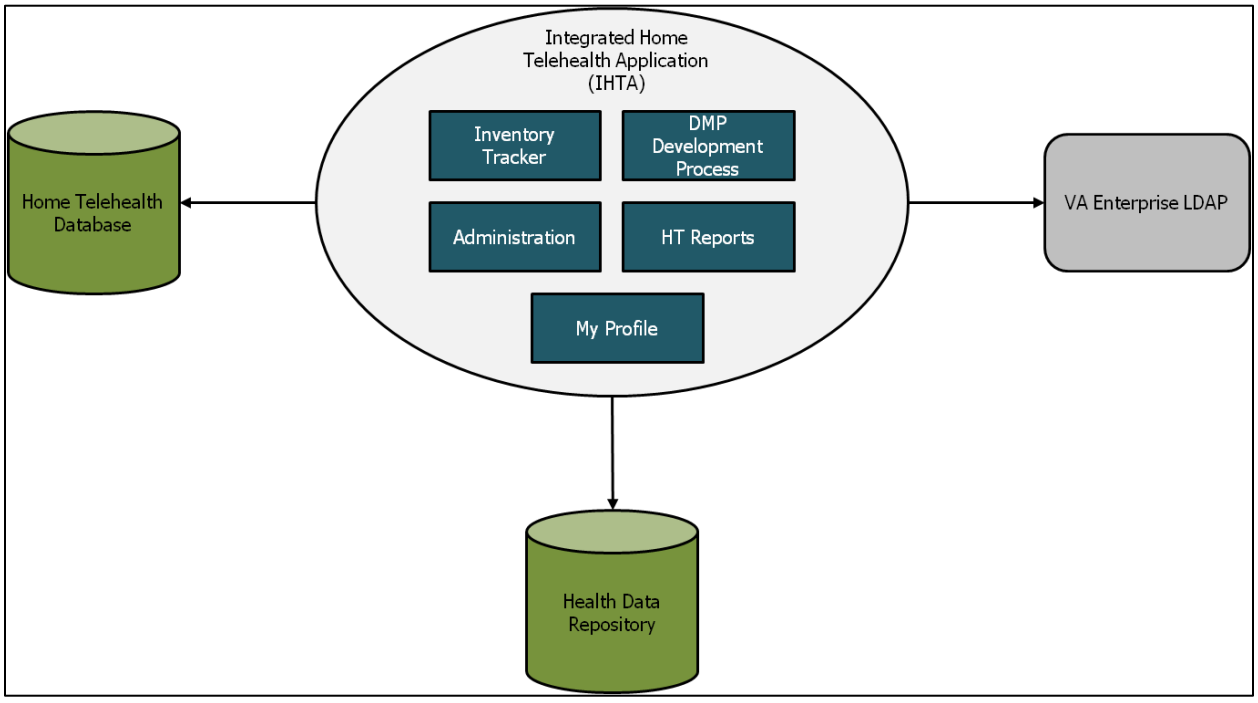

Figure 5: Dependent Systems

Table 4: Enterprise Service and Application Summary

Service	Category	Integration Technology
VA Enterprise Lightweight Directory Access Protocol (LDAP)	Authentication and Authorization	Spring LDAP
HT Database	Database for all of HT	Hibernate Java Persistence API (JPA)
Health Data Repository	System of record for HT data	HL7

2 Routine Operations

This section describes, at a high level, what is required of an operator / administrator or other non-business user to maintain the system at an operational and accessible state.

2.1 Administrative Procedures

This section describes the administrative procedures for system start-up and shut-down.

2.1.1 System Start-up

The following steps outline how IHTA is started and brought to an operational state:

Database Start-Up

1. Use system administrative techniques to validate that the database server is operational.
2. Open SQL Server Management Studio (SSMS).
3. Start the IHTA Database instance if in a non-started state.
4. Validate that the WL1035_Telehealth and Telehealth Database are running and accessible by the users.

Application Start-Up

1. Start Apache Web Server on each Web server in the cluster.
2. Start Oracle WebLogic Node Manager Service on each application server in the cluster.
3. Refer to *IHTA Installation Instructions* (Appendix A) for software installation and configuration.
4. Start Oracle WebLogic Doman for IHTA cluster.

For more detailed instructions on System Start-up, refer to Appendix A.

2.1.2 System Shut-down

The following outlines the steps for shutting down IHTA:

Application Shut-down

1. Shut down Oracle WebLogic Doman for the IHTA cluster.
2. Shut down Oracle WebLogic Node Manager Service on each application server in the cluster.
3. Shut down the Apache Web Server on each Web server in the cluster.

Database Shut-down

1. Open SSMS.
2. Shut down (stop) the IHTA Database instance.
3. Validate that the WL1035_Telehealth and Telehealth databases are no longer running.

For more detailed instructions on System Shut-down, refer to Appendix A.

2.1.3 Back-up & Restore

This section provides a high-level description of the back-up and restore strategy for IHTA.

2.1.3.1 Back-up Procedures

Refer to the *IHTA Installation Instructions* (Appendix A) for **application back-up and restore**.

For **database backup**, refer to the following:

Database Backup

The WL1035_Telehealth and Telehealth databases are backed up daily on a scheduled basis using internal database software routines A full backup is conducted in the off hours (after 6pm pacific time) for both databases . The SQL Agent job that performs all user database backups is UserDatabasesBackup.Subplan_1. Hourly transaction log backups are also scheduled for all user databases. The SQL Agent job that performs the user database transaction log backups is TeleHealthDatabaseLogBackup.Subplan 1.

All backups are performed while the database is in use. The database instance does not have to be in the shut-down state to perform any of the backups described.

The backups are stored in the following folder &files path:

- Telehealth (full): E:\SQL Backups\Telehealth\ Telehealth_backup_2015_01_06_230001_0254805.bak
- Telehealth (Transaction logs): E:\SQL Backups\LogBackups\ Telehealth\ Telehealth_backup_2015_01_06_090001_8748109.bak
- WL1035_Telehealth (full): E:\SQL Backups\WL1035_Telehealth\ WL1035_Telehealth_backup_2015_01_06_230001_0274807.bak
- WL1035_Telehealth_log_backup (Transaction logs): E:\SQL Backups\LogBackups\ Telehealth\ WL1035_Telehealth_backup_2015_01_06_090001_8768111.bak

The files should are copied to external medium and taken to an offsite location.

2.1.3.2 Restore Procedures

Refer to the *IHTA Installation Instructions* (Appendix A) for application restore procedures.

Database Restore

Database recovery should only be performed by staff experienced in database recovery techniques. The form of database recovery followed will depend on the type of database failure that required a recovery effort to be initiated.

The HT database is mirrored between two database servers (no witness). At any given time, one of the database servers serves as the primary database in support of the production application. The secondary database maintains a mirrored copy of the primary database and is kept at the same data level using replication. If the primary database loses functionality due to hardware failure, procedures should be followed that activate the secondary database server as the primary database. See the *Contingency Planning - Continuity of Operations* section of this document for the steps required to switch to the mirrored database.

Database Restore – Data Failure

Data failures will impact both the primary and secondary databases. Recovery will require full restore of the primary database from the full and transaction log file backups. The database recovery will be to a point in time prior to the start of the data failure and with minimum data loss. Refer to the *Rollback Procedures* section of this document for information on recovering the database to a prior point in time.

For more detailed instructions on restore procedures, also refer to Appendix A.

2.1.3.3 Back-up Testing

Database Restore Testing – Hardware failure

Since this type of database restore represents database server failover, it should be practiced using production. This is an exception to the normal practice of performing the testing in a separate environment. Performing database failover in production ensures that the participating environments are available to function as expected, which is not something that can be duplicated using a test environment. Database failover must be coordinated with the dependent HT applications and conducted during production off hours. To conduct the hardware failover, see the *Contingency Planning - Continuity of Operations* section of this document for the steps required to switch to the mirrored database.

Database Restore Testing – Data failure

This recovery test should be performed in a non-production environment using a SQL Server database instance of equivalent release and configuration. Perform a full recovery of the HT database using the most recent full production backup.

> Test Case #1
>
> Capture all data from the dbo.CENSUS table where the 'date_loaded' value is within ten days of the 'CURRENT_TIMESTAMP' value. Take note of the datestamp information provided. Using the date_loaded values, pick a point in time that occurs prior to the most recent value. This will be the point that you want to recover to in your practice test.

Follow the instructions for performing a point-in-time database recovery as outlined in the *Rollback Procedures* section of this document. At the completion of the recovery, test to the point in time that you picked in Test Case #1. Perform the following test case to validate your efforts:

> Test Case #2
>
> Capture all data from the dbo.CENSUS table where the 'date_loaded' value is within ten days of the 'CURRENT_TIMESTAMP' value. Take note of the information given in the 'date_loaded' column. To be successful, there should be no date_loaded values past the point in time that was picked for recovery.

2.1.3.4 Storage and Rotation

Refer to the Standard Operating Procedures (SOP) in place at the Primary and Secondary Facilities for procedures on storage and rotation.

2.2 Security / Identity Management

This section provides a high-level description of IHTA's security and user management

2.2.1 Identity Management

For VA users, the IHTA Registration Screens capture a user's VA network ID to store it in the designated IHTA database table. Once a user has registered, the application notifies the Facility / VISN Administrator and the National Administrator. The Facility, VISN, or National Administrator will approve the registration and assign roles according to the user's job description (see *IHTA Roles*). The user is then notified by e-mail that his / her registration has been approved. The screens of the Registration Approval Process capture and store IHTA database information about user roles and permissions related to the specific application module of IHTA. The table below lists the various roles and the assigned permissions.

Table 5: IHTA Permissions

Module	Permission Name
Administration	Manage Users
	Manage Roles
	Manage Batch Jobs
	Manage Registrations
Inventory Tracker	Summary Device Inventory Reports
	Search Device By Serial Number
	Search Device By Activation Date
	Vendor Compliance Reports
	Create QIR
	Update QIR
	Read QIR
	Approve QIR
	Close QIR
	Withdraw QIR
	Reply QIR
	Agree QIR
All	Administer system components
HT Reports	Generate DMP Response Reports
	Export DMP Response Reports
	Generate Patient Survey Reports
	Generate Census Activity Reports
DMP	Administer DMP Users
	Create DMP
	Update DMP
	Read DMP
	Lock-Unlock DMP Content
	Find-Replace DMP Content
	Add Comments
	View Comments
	Deploy DMP
	Create SL Content
	Update SL Content

Table 6: IHTA Roles

Role ID	Role Name	Description	Assigned Permission(s) (See Table 5, *IHTA Permissions*)	
			Module	**Permission**
2010	**Application Administrator**	An individual who is responsible for unlocking users who have locked themselves out of the application by entering their password incorrectly three times.	**Administration**	Unlock Users
2011	**National Administrator**	An individual in the Office of Telehealth Services (OTS) HT Program who is primarily responsible for the administration of IHTA.	**Administration**	• Manage Registrations • Manage Users • Manage Scheduled Jobs
			HT Reports	• Search DMP Response Reports • Export DMP Response Reports • Generate Patient Survey Reports • Generate Census Activity Reports

			Inventory Tracker	• Search Device by Serial Number
				• Search Device by Activation Date
				• Summary Device Inventory Report
				• Vendor Compliance Reports
				• Manage QIRs*
				  ○ Approve a QIR
				  ○ Read a Closed or Withdrawn QIR
				  ○ Update a QIR
				  ○ Close a QIR
				  ○ Export List of QIRs
				*The National Administrator role cannot create/withdraw a QIR in the application.

2012	**VISN Administrator**	A Care Coordinator at the VISN level who has been assigned the additional duties of supervising	**Administration**	• Manage Registrations • Manage Users

Role ID	Role Name	Description	Assigned Permission(s) (See Table 5, *IHTA Permissions*)	
			Module	**Permission**

		the administration of IHTA for the VISN.	**Inventory Tracker**	• Search Device by Serial Number
				• Search Device by Activation Date
				• Summary Device Inventory Report
				• Vendor Compliance Reports
				• Manage QIRs
				  ○ Create a QIR
				  ○ Agree to a Vendor's response to a QIR
				  ○ Withdraw a QIR
				  ○ Update a QIR
				  ○ Read a Closed or Withdrawn QIR

			HT Reports	All functionality
2013	**Facility Administrator**	A Care Coordinator at a facility who has been assigned the additional duties of supervising the administration of IHTA for that facility.	**Administration**	• Manage Registrations • Manage Users
			Inventory Tracker	• Search Device by Activation Date • Search Device by Serial Number • Summary Device Inventory Report • Vendor Compliance Reports
			HT Reports	All functionality
2014	**Care Coordinator**	A registered nurse who manages care across the health care continuum for a panel of HT patients.	**Inventory Tracker**	• Search Device by Activation Date • Search Device by Serial Number

Role ID	Role Name	Description	Assigned Permission(s) (See Table 5, *IHTA Permissions*)	
			Module	**Permission**
				• Summary Device Inventory Reports
			HT Reports	All functionality
2015	**Program Support Assistant**	An individual who is responsible for establishing and maintaining inventory of all HT equipment at the facility.	**Inventory Tracker**	• Search Device by Activation Date • Search Device by Serial Number ▪ Summary Device Inventory Reports
			HT Reports	All functionality
2016	**Management**	A headquarters level individual who uses IHTA reports and information to support HT Program activities.	**Inventory Tracker**	• Summary Device Inventory Reports • Vendor Compliance Reports
			HT Reports	• Generate DMP Response Reports • Export DMP Response Reports • Generate Patient Survey Reports • Generate Census Activity Reports
2017	**Vendor**	One or more individuals who are the authorized representative for a supplier of HT equipment.	**Inventory Tracker**	• Manage QIRs ○ Read a QIR ○ Reply to a QIR ○ Update a QIR
2018	**OTS Contract Manager**	Office of Telehealth Service (OTS) Contract Manager	**Inventory Tracker**	• Manage QIRs ○ Read a QIR
			HT Reports	• All Functionality
2019*	**Clinical Analyst**	An individual in the OTS HT Program who is responsible for providing clinical advice on HT issues.	**Administration**	• Manage Registrations • Manage Users • Manage Scheduled Jobs
			Inventory Tracker	• Search Device by Serial Number • Search Device by Activation

Role ID	Role Name	Description	Assigned Permission(s) (See Table 5, *IHTA Permissions*)	
			Module	**Permission**
				• Date • Summary Device Inventory Report • Vendor Compliance Reports
2020	**System Administrator**	An individual assigned to be a super user of IHTA with access to all functionality in IHTA.	**Administration, Inventory Tracker, DMP Development Process, HT Reports**	• All functionality
2022	**QIR Originator**	An individual responsible for submitting Quality Improvement Reports (QIR) in the application to document quality and patient safety issues related to HT devices.	**Inventory Tracker**	• Create QIR • Update QIR • Agree QIR • Withdraw QIR • Read QIR
			HT Reports	• All Functionality
2023	**DMP Contributor**	An individual assigned to contribute content to a DMP (e.g., questions, responses, educational content, etc.) created in the DMP module.	**DMP**	• Update DMP • Read DMP • View My • Search All • Find Content • Add Comment (if assigned as a DMP Reviewer) • View Comments (if assigned as DMP Reviewer)
2023 2024	**DMP Contributor** **DMP Administrator**	An individual assigned to contribute content to a DMP (e.g., questions, responses, educational content, etc.) created in the DMP module. An individual within the Home Telehealth National Training Center (HTNTC) who is responsible for managing all DMPs assigned to users in the DMP module.	**HT Reports**	• All functionality
			Administration	• Manage Registrations Manage Users

Role ID	Role Name	Description	Assigned Permission(s) (See Table 5, *IHTA Permissions*)	
			Module	**Permission**
2024	**DMP Administrator**	An individual within the Home Telehealth National Training Center (HTNTC) who is responsible for managing all DMPs assigned to users in the DMP module.	**HT Reports**	• All functionality
			DMP	• Create DMP • Update DMP • Assign User • Remove Users • Assign DMP Reviewer role • Remove DMP Reviewer role • Edit DMP • View My • Read DMP • Export DMP • Find-Replace Content • Lock-Unlock DMP Content • Search All • Create SL Content • Update SL Content • Read SL Content • Deploy DMP • Add Comment View Comments
			Inventory Tracker	• All Functionality
				•

*NOTE**:** The *Clinical Analyst* role listed in Table 6 was removed from the database in January 2012 per request by the customer (refer to CCR 641 in ClearQuest).

2.2.2 Access Control

VA network credentials are used for access control. The IHTA architecture leverages the existing Java Authentication & Authorization Service (JAAS) to authenticate VA users against the VA Enterprise LDAP.

Access to IHTA will be granted upon successful authentication against the existing VA Enterprise LDAP. It is important to note that logging into IHTA will not grant access to all application modules or embedded systems in IHTA. There will be authorizations that govern access to each of the application modules or embedded systems. There will also be authorizations that govern access within each application module.

IHTA will authenticate its users against the VA Enterprise LDAP, but not implement direct Security Assertion Mark-up Language (SAML). Since users at each VA Medical Center (VAMC) are present in LDAP at the VISN level (e.g., vXX.med.va.gov, etc.), IHTA will establish a one-way trust with the VA Enterprise LDAP. This will allow all VISN users' access to IHTA.

2.3 User Notifications

All routine IHTA maintenance will be performed off-hours (not during the normal work week of Monday through Friday) to minimize impact to IHTA users. A System 404 message, "Application Out of Order", will display when a user attempts to log into IHTA and the application is down. In cases of an extended unscheduled system outage, the IHTA Administrator will distribute a notification via e-mail as soon as practicable notifying all users of the system outage and the efforts being made to correct it. A second e-mail will be distributed when the system has returned to a normal operational state (refer to Table 7).

Table 7: IHTA Outage E-mails

1 - Extended Unscheduled System Outage
TO: <HT/CCHT VISN and Facility Leads, Care Coordinators, Program Support Assistants> **FROM:** IHTA Support **RE:** URGENT: IHTA Unavailable - Unscheduled System Outage The Integrated Home Telehealth Application (IHTA) is currently down. The IHTA Support staff is currently researching the issue. Please look for another e-mail when the application has returned to an operational state. **IHTA Support Team**
2 - Status Update – System Outage (After 4 Hours) (If Applicable)
TO: <HT/CCHT VISN and Facility Leads, Care Coordinators, Program Support Assistants> **FROM:** IHTA Support **RE:** URGENT: Status Update – IHTA Outage The Integrated Home Telehealth Application (IHTA) continues to be down. The IHTA Support staff continues to research the issue. Please look for another e-mail when the application has returned to an operational state. **IHTA Support Team**
3 – Outage Resolved
TO: <HT/CCHT VISN and Facility Leads, Care Coordinators, Program Support Assistants> **FROM:** IHTA Support **RE: URGENT:IHTA Now Available - Outage Resolved** The Integrated Home Telehealth Application (IHTA) is now available. The outage has been resolved. Please contact the IHTA Support Team if you experience any issues with accessing the application. **IHTA Support Team**

2.3.1 Unscheduled System Outage Procedure

1. The IHTA Support Team is notified that the application is unavailable.

2. After being notified, the IHTA System Administrator (SA) verifies the unscheduled outage.

3. The IHTA Support Team sends the **Extended Unscheduled System Outage** e-mail message to the VISN, Facility, and National Administrators (see Table 7). The following subject line is used in the e-mail:

   URGENT: IHTA Unavailable – Unscheduled IHTA Outage

4. The VISN and Facility Administrators notify their users that IHTA is unavailable and keep them apprised as they receive status updates.

5. The IHTA SA researches the problem and either resolves it or escalates it to the HT SA and/or HT Database Administrator (DBA).

6. The IHTA SA sends the **Outage Status Update** (see Table 7) e-mail message to the VISN and Facility Administrators and the National Administrator. The message is sent when the technical staff has an estimated time of system restoration or when four hours has passed since the prior message, whichever comes first.

7. The following subject line is used in the **Outage Status Update** e-mail message:

   URGENT: Status Update – IHTA Outage

8. When the problem is resolved, the IHTA SA sends the **Outage Resolved** e-mail message to the VISN and Facility Administrators and the National Administrator (see Table 7). The following subject line is used in the e-mail:

   URGENT: IHTA Now Available – Outage Resolved

Refer to the *Home Telehealth O&M Plan*. Also, refer to the SOPs, Disaster Recovery Plans (DRP), and Contingency Plans at the Primary and Secondary Facilities for the standard user notifications in effect.

2.4 System Monitoring, Reporting & Tools

Only rudimentary system monitoring and reporting techniques (e.g., ping, manual logins, etc.) are being employed for IHTA as described in the below subsections. The IHTA SA and DBA are responsible for system monitoring. As of this release, no formal monitoring tools are being utilized.

2.4.1 Availability Monitoring

The IHTA SA utilizes a Multi-Routing Tracking Grapher (MRTG) (see link below) for determining the overall operational state of IHTA.

Base URL: http://vaww-dashboard.ciss.cc.med.va.gov/mrtg/

htiew001_2.html	htiew001_cpu.html	htiew001_mem.html	vhaiswhtied102_10.2.54.148.html

2.4.2 Performance/Capacity Monitoring

IHTA monitors system performance utilizing an At-a-Glance Report e-mailed daily by AITC. The report provides details on Total Packets/Second, CPU Utilization, Total Common Errors, Interface Utilization, Virtual Memory Utilization, Pages Swapped, and Latency.

2.4.3 Critical Metrics

IHTA utilizes the At-a-Glance Report e-mailed daily by AITC for critical metrics important to validating normal operations.

2.5 Routine Updates, Extracts and Purges

Database updates and manual extracts are currently performed manually by the DBA upon request. Automate data extracts in support of Inventory Tracker are completed weekly. Any required database reorganizations and data purges will be done manually by the HTRE DBA.

2.6 Scheduled Maintenance

Following the VA's Monthly OS patching Schedule , the SA, in collaboration with the IHTA Development team, verifies and updates (as required) operating system (OS) patches. All necessary IHTA production maintenance will be performed during off-hours. A "System Not Available" page displays when the application is down. Also, refer to the SOPs in place at the Primary and Secondary facilities.

2.7 Capacity Planning

HTRE will perform a capacity review as part of the planning for each release at six-month intervals. The HTRE-IHTA SA/HT DBA will be responsible for these reviews.

2.7.1 Initial Capacity Plan

Existing capacity has been deemed adequate for this release of IHTA.

3 Exception Handling

This section provides a high-level overview of how system problems are handled.

3.1 Routine Errors

Like most systems, IHTA may generate a small set of errors that may be considered routine in the sense that they have minimal impact on the user and do not compromise the operational state of the system. Most of the errors are transient in nature and only require the user to retry an operation. The following subsections describe these errors, their causes, and what, if any, response an operator needs to take.

While the occasional occurrence of these errors may be routine, getting a large number of an individual error over a short period of time is an indication of a more serious problem. In that case the error needs to be treated as an exceptional condition.

3.1.1 Security Errors

Please refer to Section 3.2.3.. Authentication and Authorization, for the security errors related to registration and login.

3.1.2 Time-outs

The application automatically logs a user out after 15 minutes of inactivity. Note that this is a system feature, not an error, but is mentioned here for completeness. A warning message

displays, counting down from 60 seconds or until the user logs off the application. A user can click the **OK** button to stop the countdown and continue working.

3.1.3 Concurrency

As a Web-based application, IHTA allows users to share data in a multi-user environment. Data is stored in database tables on a database server (Microsoft SQL Server). In a multi-user environment, more than one person may work with the same record at the same time. Since other users can change or even delete the same data that another user is trying to edit, users may occasionally conflict with others as they work. IHTA keeps track of the status of records as users edit them, and makes sure a user is using the latest data. When two or more people try to edit the same record, IHTA will display a suitable error message to assist with resolving the conflict. In most cases, users will respond to one of these errors by attempting their action again. The concurrency errors in IHTA include the following:

- **optimistic.locking.text**=Database operation failed because object was changed by another session. You will have to re-load it and re-apply your changes.
- **optimistic.locking.title**=Optimistic Locking Error
- **patient.optimistic.locking.text**=Changes to record could not be saved because it was changed by another user. Please re-submit.
- **role.optimistic.locking.text**=Changes to role could not be saved because it was changed by another user. Please re-submit.

3.2 Significant Errors

Significant errors can be defined as errors or conditions that affect the system stability, availability, performance, or otherwise make the system unavailable to its user base. The following subsections contain information to aid administrators, operators, and other support personnel in the resolution of errors, conditions, or other issues.

3.2.1 Application Error Logs

Tool: Text editor

Name/Location: DOMAIN_HOME/ccht.log

Configuration file: /ccht_common/src/main/resources/env/ccht_log4j.xml

Info from configuration file:

Max size: 10MB

Growth rate: dependent on log level. Default is ERROR with negligible growth.

Rotation: after Max file size is reached

Retention: 10 iterations of rotation.

Specific configuration from ccht_log4j.xml:

```
        <appender name="ccht.file.appender.detailed"
class="org.apache.log4j.RollingFileAppender">
            <param name="append" value="true" />
            <param name="file" value="ccht.log" />
            <param name="maxFileSize" value="10MB" />
            <param name="maxBackupIndex" value="10" />
            <layout class="org.apache.log4j.PatternLayout">
```

```
                <param name="ConversionPattern" value="[%p] %d{yyyyMMdd hh:mm:ss aa SSS} %t
[%c]%n%m%n%n" />
            </layout>
        </appender>
```

3.2.2 Application Error Codes and Descriptions

Refer to Appendix A and B for a complete list of all errors generated by the application.

3.2.3 Infrastructure Errors

The following subsections outline the errors for the various components of IHTA.

3.2.3.1 Database

IHTA processing will include exception handling of database errors, providing user feedback, and logging the error on the application server for troubleshooting support and process traceability.

The HT database is configured to log the appropriate level of detail when an error occurs. Staff administrators will use the logged error information to conduct an evaluation of the database error and perform resolution to make the database software or hardware operational.

3.2.3.2 Web Server

The two log files for the IHTA Web Server are listed below:

1. **access_log**: Logs information related to general IHTA access (e.g., IP address, user, timestamp, etc.).
2. **error_log**: Logs error information related to displaying an IHTA Web page.

Also, refer to the log files for the VA Enterprise LDAP and the HT Database.

3.2.3.3 Application Server

On each application server cluster, errors are logged into a set of log files for each managed server. The seven log files and their descriptions are listed below:

1. The **ccht.log** file contains log information generated by the IHTA application codes.
2. The **MS1.log** file contains log information generated by the Manage Server 1.
3. The **MS1.out** file contains log information directed to the console output of Manage Server 1.
4. The **MS2.log** file contains log information generated by the Manage Server 2.
5. The **MS2.out** file contains log information directed to the console output of Manage Server 2.
6. The **adminServer.log** contains log information generated by the Admin Server.
7. The **adminServer.out** contains log information directed to the console output of the Admin Server.

3.2.3.4 Network

The following Linux commands are used for identifying errors and resolving network errors:

Command in **BOLD BLACK**
Command prompt in light grey
Output from command in red.
Highlighted are key areas to look for Possible problems.
BLUE UPPERCASE ITALIC are comments

```
[root@vhacrbwebihta91 ~]# mii-tool -v
      eth0: negotiated 100baseTx-FD, link ok
        product info: vendor 00:50:ef, model 60 rev 8
        basic mode:   autonegotiation enabled
        basic status: autonegotiation complete, link ok
        capabilities: 100baseTx-FD 100baseTx-HD 10baseT-FD 10baseT-HD
        advertising:  100baseTx-FD 100baseTx-HD 10baseT-FD 10baseT-HD flow-
      control
        link partner: 100baseTx-FD 100baseTx-HD 10baseT-FD 10baseT-HD
      eth1: no link - This could be a Problem if there was an expectation of
      a ethernet connection established, not an issue in this case, no
      ethernet connected to this NIC
        product info: vendor 00:50:ef, model 60 rev 8
        basic mode:   autonegotiation enabled
        basic status: no link
        capabilities: 100baseTx-FD 100baseTx-HD 10baseT-FD 10baseT-HD
        advertising:  100baseTx-FD 100baseTx-HD 10baseT-FD 10baseT-HD flow-
      control

[root@vhacrbwebihta91 ~]# ethtool eth0
      Settings for eth0:
              Supported ports: [ TP ]
              Supported link modes:   10baseT/Half 10baseT/Full
                                      100baseT/Half 100baseT/Full
                                      1000baseT/Full
              Supports auto-negotiation: Yes
              Advertised link modes:  10baseT/Half 10baseT/Full
                                      100baseT/Half 100baseT/Full
                                      1000baseT/Full
              Advertised auto-negotiation: Yes
              Speed: 1000Mb/s
              Duplex: Full  - This could be a Problem if set to Half.
              Port: Twisted Pair
              PHYAD: 1
              Transceiver: internal
              Auto-negotiation: on
              Supports Wake-on: g
              Wake-on: d
              Link detected: yes

[root@vhacrbwebihta91 ~]# lsof -Pni; ###   Depending on the issue, the
output is important
      COMMAND    PID        USER   FD   TYPE  DEVICE SIZE/OFF NODE NAME
      httpd     2878      apache    3u  IPv6   15015      0t0  TCP *:80 (LISTEN)
      httpd     4429      apache    3u  IPv6   15015      0t0  TCP *:80 (LISTEN)
      portmap   4653         rpc    3u  IPv4    9593      0t0  UDP *:111
      portmap   4653         rpc    4u  IPv4    9594      0t0  TCP *:111 (LISTEN)
```

```
sshd      4725         root    3u  IPv4 1857407      0t0  TCP XXX.XXX.XXX.XX:22-
>YYY.YYY.YYY.YYY:55277 (ESTABLISHED)
rpc.statd 4734      rpcuser    3u  IPv4    9894      0t0  UDP *:673
rpc.statd 4734      rpcuser    6u  IPv4    9884      0t0  UDP *:670
rpc.statd 4734      rpcuser    7u  IPv4    9905      0t0  TCP *:676 (LISTEN)
hpiod     6351         root    0u  IPv4   14654      0t0  TCP 127.0.0.1:2208 (LISTEN)
hpssd.py  6356         root    4u  IPv4   14672      0t0  TCP 127.0.0.1:2207 (LISTEN)
sshd      6369         root    3u  IPv6   14708      0t0  TCP *:22 (LISTEN)
cupsd     6378         root    4u  IPv4   14750      0t0  TCP 127.0.0.1:631 (LISTEN)
ntpd      6403          ntp   17u  IPv6   14822      0t0  UDP *:123
ntpd      6403          ntp   18u  IPv6   14823      0t0  UDP
[fe80::7a2b:cbff:fe24:4e68]:123
ntpd      6403          ntp   19u  IPv6   14824      0t0  UDP [::1]:123
ntpd      6403          ntp   20u  IPv4   14825      0t0  UDP 127.0.0.1:123
ntpd      6403          ntp   22u  IPv4   14827      0t0  UDP  XX,XXX,XXXX,XXX,XX69:123
sendmail  6421         root    4u  IPv4   14917      0t0  TCP 127.0.0.1:25 (LISTEN)
snmpd     6733         root    9u  IPv4   15632      0t0  TCP 127.0.0.1:199 (LISTEN)
snmpd     6733         root   10u  IPv4   15633      0t0  UDP *:161
snmpd     6733         root   12u  IPv4   16481      0t0  TCP 127.0.0.1:199-
>127.0.0.1:50913 (ESTABLISHED)
dsm_sa_sn 6989         root    4u  IPv4   16480      0t0  TCP 127.0.0.1:50913-
>127.0.0.1:199 (ESTABLISHED)
```

```
[root@vhacrbwebihta91 ~]# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 78:2B:CB:24:4E:68
          inet addr:XX.XXX.XXXX.XXX.XX Bcast:XX.XXX.XXXX.XXX.XX Mask:255.255.255.192
          inet6 addr: fe80::7a2b:cbff:fe24:4e68/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2573375 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2565790 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:211822483 (202.0 MiB)  TX bytes:324341582 (309.3 MiB)
          Interrupt:98 Memory:d6000000-d6012800

eth1      Link encap:Ethernet  HWaddr 78:2B:CB:24:4E:69
          inet addr:XX.XXX.XXXX.XXX.XX Bcast:XX.XXX.XXXX.XXX.XX Mask:255.255.255.192
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:106 Memory:d8000000-d8012800
```

```
[root@vhacrbwebihta91 ~]# ethtool -S eth0
NIC statistics:
     rx_bytes: 211807772
     rx_error_bytes: 0
     tx_bytes: 324314543
     tx_error_bytes: 0
     rx_ucast_packets: 2568178
     rx_mcast_packets: 0
     rx_bcast_packets: 4993
     tx_ucast_packets: 2565576
     tx_mcast_packets: 6
     tx_bcast_packets: 3
     tx_mac_errors: 0
     tx_carrier_errors: 0
     rx_crc_errors: 0
     rx_align_errors: 0
     tx_single_collisions: 0
     tx_multi_collisions: 0
     tx_deferred: 0
     tx_excess_collisions: 0
     tx_late_collisions: 0
     tx_total_collisions: 0
     rx_fragments: 0
     rx_jabbers: 0
     rx_undersize_packets: 0
     rx_oversize_packets: 0
     rx_64_byte_packets: 423920
```

```
rx_65_to_127_byte_packets: 2109535
rx_128_to_255_byte_packets: 17144
rx_256_to_511_byte_packets: 491
rx_512_to_1023_byte_packets: 1241
rx_1024_to_1522_byte_packets: 20840
rx_1523_to_9022_byte_packets: 0
tx_64_byte_packets: 420077
tx_65_to_127_byte_packets: 1708868
tx_128_to_255_byte_packets: 11393
tx_256_to_511_byte_packets: 422519
tx_512_to_1023_byte_packets: 886
tx_1024_to_1522_byte_packets: 1842
tx_1523_to_9022_byte_packets: 0
rx_xon_frames: 0
rx_xoff_frames: 0
tx_xon_frames: 0
tx_xoff_frames: 0
rx_mac_ctrl_frames: 0
rx_filtered_packets: 1740100
rx_ftq_discards: 0
rx_discards: 0
rx_fw_discards: 0
```

```
[root@vhacrbwebihta91 ~]# ping vha.med.va.gov;
PING vha.med.va.gov (XXX.XXX.XXX.XXX) 56(84) bytes of data.
64 bytes from vhaxxxxdcv1.vha.med.va.gov (XXX.XXX.XXX.XXX): icmp_seq=1 ttl=119 time=11.0
ms
64 bytes from vhaxxxxdcv1.vha.med.va.gov (XXX.XXX.XXX.XXX): icmp_seq=2 ttl=119 time=13.7
ms

--- vha.med.va.gov ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 11.037/12.398/13.760/1.366 ms
```

Depending on the time in ms, greater than 70-100 is minor concern, 100+ is medium concern, 150+ beginning of major network latency issues.
Same applies to the traceroute command.

```
[root@vhacrbwebihta91 ~]# traceroute <HOSTNAME/IP>
```

3.2.3.5 Authentication & Authorization

The following tables lists IHTA-specific implementation of the authentication and authorization component(s) as it relates to errors, error reporting, and other pertinent information on causes and remedy of errors.

Table 8: IHTA Authentication & Authorization

Action	Error Message
IHTA Registration	
User enters a invalid VA user name when	user.notfound=Invalid User Name.
User has previously registered and tries to register again	user.found=User Name already exists. Please contact your Facility Administrator. registration.approved=You have previously registered. Your registration was approved. Click here to login
User has previously registered, registration was denied, and tries to register again	registration.denied=You have previously registered. Your registration was denied. Please contact your Facility Administrator.
User has previously registered, the registration has not been approved, and tries to register again	registration.pending=You have previously registered. Your registration is pending. Please contact your Facility Administrator.
IHTA Login	
User does not enter VA user name	username.required=User Name is required
User does not enter password	password.required=Password is required.
User enters invalid user name or password	account.notfound=Invalid User Name or Password. bad.credentials=Invalid User Name or Password.
User is locked out of the system and tries to log in	account.locked=You are currently locked out of the system. Please contact your Facility Administrator.
User is inactive in the system and tries to log in	account.inactive=You are currently inactive in the system. Please contact your Facility Administrator.
User has not registered nor has been approved and tries to log in	insufficient.privileges=You are not authorized to login to IHTA. Please contact your Facility Administrator.

3.3 Dependent System(s)

Dependent system errors are handled by the groups responsible for those systems by referring to the HDR and VA Enterprise LDAP logs. IHTA support personnel will need to contact these other teams to report such errors and obtain resolution.

For HDR, the IHTA SA/DBA contacts the following:

Mark Broda, HDR Functional Analyst
Mark.Broda@va.gov
317-742-7619

As a general rule, if LDAP is down then there is nothing that the IHTA team can do until LDAP returns to an operational state. For user-specific LDAP issues, the IHTA team will contact the

National Service Desk – Tuscaloosa (NSD) and open a Remedy ticket (or direct the user to contact NSD).

3.4 Troubleshooting

This section provides general guidelines for trouble shooting the IHTA system.

3.5 System Recovery

The following subsections define the process and procedures necessary to restore the system to a fully operational state after a service interruption. Each of the subsections starts at a specific system state and ends up with a fully operational system.

3.5.1 Restart after Non-Scheduled System Interruption

This section describes the restart of the system after the crash of the main application.

3.5.2 Restart after Database Restore

This section describes how to restart the system after restoring from a database backup.

Database Start-Up

1. Open SQL Server Management Studio (SSMS).
2. Start the IHTA Database instance.
3. Validate that the WL1035 Telehealth and Telehealth Database are running and accessible by the users.

Application Start-Up

1. Start Apache Web Server on each Web server in the cluster.
2. Start Oracle WebLogic Node Manager Service on each application server in the cluster.
3. Refer to *IHTA Installation Instructions* (Appendix A) for software installation and configuration.
4. Start Oracle WebLogic Doman for IHTA cluster.

3.5.3 Back Out Procedures

This section outlines the back out procedures for IHTA.

3.5.3.1 Rollback ccht.ear on WebLogic Portal Server

The following are the steps to rollback ihta.ear deployed on IHTA domain to its previous version:

1. Log onto **vhacrbappihta91.HTRE.cc.med.va.gov** as wlp_user user

2. Locate the backup version of ccht.ear .<version number> under **/u01/domains/ihta_prod/appStage/**

3. Change the backup version of ccht.ear .<version number> under ccht.ear

4. Run the following command to un-deploy the current version of ccht.ear from IHTA cluster of Managed Servers configured in IHTA Domain "**~/bin/stopcluster.sh ~/ prod.properties ; ~/bin/undeploy.sh ~/prod.properties**"

5. Wait for the script to complete successfully to proceed to the next step. Contact IHTA System Administrator if you encounter problems.

6. Run the following command to deploy the previous version of ccht.ear onto IHTA cluster of Managed Servers configured in IHTA Domain "**~/bin/deploy.sh prod.properties /u01/domains/ihta_prod/appStage/ccht.ear; ~/bin/startcluster.sh ~/ prod.properties**"

7. Wait for the script to complete successfully to proceed to the next step. Contact the IHTA System Administrator if you encounter problems.

8. Open a browser to access https://vaww.htie.cc.med.va.gov/ccht/ to check if the deployment completed successfully

3.5.3.2 Rollback static contents on Apache Web Server

The following are the steps to rollback IHTA static content to their previous versions:

1. Log onto **vhacrbwebihta91.HTRE.cc.med.va.gov** as ihta user.

2. Traverse to /tmp directory and rename the following files: admin.zip, hdi.zip, main.zip, profile.zip, qir.zip, ihta.zip, register.zip, dmp.zip, and reports.zip to admin.zip.<version number>, hdi.zip.<version number>, qir.zip.<version number>, ihta.zip.<version number>, main.zip.<version number>, profile.zip.<version number>, register.zip.<version number>, dmp.zip. <version number>, and reports.zip <version number>.

3. Rename the following backup files: admin.zip.<version number>, hdi.zip.<version number>, main.zip.<version number>, profile.zip.<version number>, qir.zip.<version number>, ihta.zip.<version number>, register.zip.<version number>, dmp.zip. <version number>, and reports.zip. <version number> to admin.zip, hdi.zip, main.zip, profile.zip, register.zip, dmp.zip, and reports.zip.

4. Run the following command to deploy the previous version of IHTA static content files onto **vhacrbwebihta91** server "**~/bin/deploy.sh ~/prod.properties help**"

5. Log onto **vhacrbwebihta92.HTRE.cc.med.va.gov** as ihta user

6. Traverse to /tmp directory and rename the following files: admin.zip, hdi.zip, main.zip, profile.zip, qir.zip, ihta.zip, register.zip, and dmp.zip to admin.zip.<version number>, hdi.zip.<version number>, qir.zip.<version number>, ihta.zip.<version number>, and main.zip.<version number>, profile.zip.<version number>, register.zip.<version number>, dmp.zip. <version number>, and reports.zip <version number>.

7. Rename the following backup files: admin.zip.<version number>, hdi.zip.<version number>, main.zip.<version number>, profile.zip.<version number>, qir.zip.<version

number>, ihta.zip.<version number>, register.zip.<version number>, dmp.zip. <version number>, and reports.zip <version number> to admin.zip, hdi.zip, main.zip, profile.zip, register.zip, dmp.zip, reports.zip.

8. Run the following command to deploy the previous version of the IHTA static content files onto vhacrbwebihta91 server "~/bin/deploy.sh ~/prod.properties help"

9. Open a browser and check the following links to verify that the deployment completed successfully for the five help files:

Main IHTA Help File	ihta.zip	https://vaww.htie.cc.med.va.gov/help/ihta/
Administration Help File	admin.zip:	https://vaww.htie.cc.med.va.gov/help/admin/
Inventory Tracker Help File	hdi.zip:	https://vaww.htie.cc.med.va.gov/help/hdi/
QIR Help	qir.zip	https://vaww.htie.cc.med.va.gov/help/qir
Login Issues Help File	main.zip:	https://vaww.htie.cc.med.va.gov/help/main/
Registration Help File	register.zip:	https://vaww.htie.cc.med.va.gov/help/register/
My Profile Help File	profile.zip:	https://vaww.htie.cc.med.va.gov/help/profile/
DMP Help File	dmp.zip	https://vaww.htie.cc.med.va.gov/help/dmp/
HT Reports Help File	reports.zip	https://vaww.htie.cc.med.va.gov/help/reports/

3.5.4 Rollback Database Procedures

Recovery of the database to a prior point in time will require restoring the database from a full backup and applying the transaction logs necessary to bring the database state to the point in time decided upon. All due consideration should be given to the impact that this form of database recovery will have as data will be lost. Performing a database rollback recovery should only be considered after all other possible approaches to data correction have been found to have a greater impact than a point-in-time recovery. The following subsections describe the process for rolling back a database to a desired point in time.

3.5.4.1 Backup Selection

Select the full database backup that is prior to and closest to the point in time that the database will be recovered to. If the backup is on external medium, transfer it to a folder on the primary database server so that it is directly available to the database software. Select all transaction log backups that were taken 24 hours prior to the database backup you have selected, and all transaction log backups taken up to and includes the point in time that you have targeted, to recover the database to. If the transaction log backups are on external medium, transfer all to a folder on the primary database server so that they are directly available to the database software.

3.5.4.2 Database Recovery Preparation

1. Make sure all application use of the database is shutdown. Place the database in the restricted access mode and clear all current user connections.

2. Shutdown mirroring. Since the secondary database is also affected by the same data issue that is impacting the primary, the mirroring database will need to be rebuilt once the recovery is completed.
3. Though it is the database that needs to be corrected, it also represents the starting point if the recovery effort fails for any reason. Take a full backup of the database. Save the backup in a file just in case it is needed to rebuild and restart the recovery.

3.5.4.3 Database Point in time Restore

1. Connect to the appropriate instance of the Microsoft SQL Server Database Engine.
2. Expand **Databases** and select the database to be recovered.
3. Right-click the database, point to **Tasks**, and then click **Restore**.
4. Click **Database**.
5. On the **General** page, the name of the restoring database appears in the **To database** list box. To create a new database, enter its name in the list box.
    - For the point-in-time option pick **Restore Database:** The **To a point in time** option is in the **Destination for restore** section.
6. In the **Point in Time Restore** dialog box, click **A specific date and time**.
    - In the **Date** list box, enter or select a date.
    - In the **Time** list box, enter or select a time.
7. To specify the source and location of the backup sets to restore, select **From device.** Click the browse button and identify the location of the full database and transaction log files that you created earlier. Click **OK** to return to the **General** page.
8. After you have specified a specific point in time, only the backups that are required to restore to that point in time are selected in the **Restore** column of the **Select the backup sets to restore** grid. These selected backups make up the recommended restore plan for your point-in-time restore. You should use only the selected backups for your point-in-time restore operation.
9. In the **Restore options** panel, you choose '**Overwrite the existing database**', '**Preserve the replication settings'** and '**Restrict access to the restored database'.**
10. The **Recovery state** panel determines the state of the database after the restore operation. Keep the default behavior which is:
    - **Leave the database ready for use by rolling back the uncommitted transactions. Additional transaction logs cannot be restored. (RESTORE WITH RECOVERY)**
11. Start the database recovery.

3.5.4.4 Database Recovery Follow-up – Restart mirroring; open database to user access

1. Create a full database backup and a backup of the transaction log.
2. Copy the backups to the secondary database server.
3. Perform the steps above to recover the database on the secondary database server but with the options:

- Restore the database backup without recovering the database (RESTORE DATABASE database_name FROM backup_device WITH NORECOVERY).
- Continue with the transaction log backup that was created after the backup you just restored, (RESTORE the logs in sequence with NORECOVERY).
- You want the database to end up in a 'restoring state'.

4. On the primary server, take steps to start database mirroring between the primary and secondary servers.
5. Remove the restricted user access to the primary database.

4 Operations & Maintenance System Support

An understanding of how IHTA is supported by various organizations within the VA is important to operators and administrators of the system. If you are unable to resolve an issue, then it is necessary to understand how to obtain support through OIT's system support organizations. The following sections describe the support structure and provide procedures on how to obtain support.

The Operations and Maintenance (OM) section defines the roles and responsibilities of each party involved in the delivery and support of the application/service. Precise definition of roles and responsibilities is necessary in a typical shared responsibility environment to avoid confusion over which party is responsible for a specific task or action.

It is not necessary to restate and redefine roles and responsibilities in the OM section for conventional products and services in the Service Strategy and Service Design activities, as they are known. It is only necessary to explicitly state roles and responsibilities in the Service Operation and Continued Service Improvement activities.

Once participating offices have been identified as having an active role in the Operations and Maintenance of IHTA, columns in the linked matrix should be reviewed, updated, and removed as necessary. A detailed RACI (R – Responsible A- Accountable, C – Consulted, I – Informed) Matrix is to be developed for each OM section to show specific roles and responsibilities by environment.

IHTA_O&M_Responsibility_Matrix.xls

4.1 Support Structure

This section describes the systems support structure as seen from the perspective of operations personnel. The first section defines the support hierarchy through which a support request may navigate. The second section defines the responsibilities for each level of support.

4.1.1 Support Hierarchy

Support for IHTA will be provided by the NSD utilizing the Remedy Help Desk. Tier 1, 2, and 3 support will be performed by the groups indicated in Figure 6.

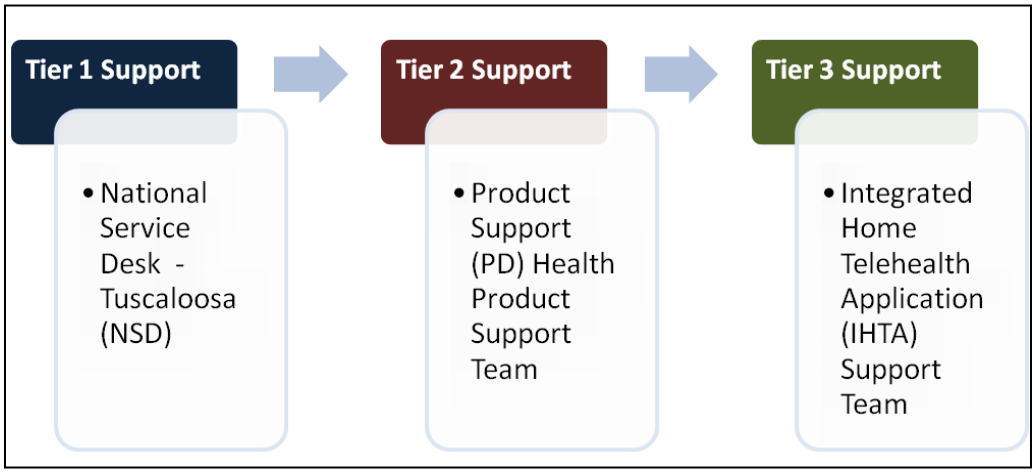

Figure 6: Overview of IHTA Support

4.1.2 Division of Responsibilities

Tier 1 Support: NSD; Tier 2 Support: Health Product Support; Tier 3 Support: IHTA Support Team

4.2 Support Procedures

Tier 1 Support will be provided by the NSD utilizing the Remedy system. IHTA users with problems that cannot be resolved locally will call the NSD to open a Remedy ticket. Issues not resolved by the Tier 1 Support Team will be assigned to Tier 2 Support in Remedy. Tier 2 Support for IHTA will include assistance from the PD Product Support Team. Issues not resolved by the Tier 2 Support Team will be assigned to Tier 3 Support in Remedy. Tier 3 Support is the highest level of support for IHTA, which includes business analysts, software testers, system administrators, developers, and database administrators who have specialized technical knowledge of IHTA (see Figure 7). Tier 3 Support will resolve all issues/defects that have not been resolved by the Tier 1 and 2 Support Teams. Issues identified in Remedy tickets may also be logged in Rational ClearQuest (as required).

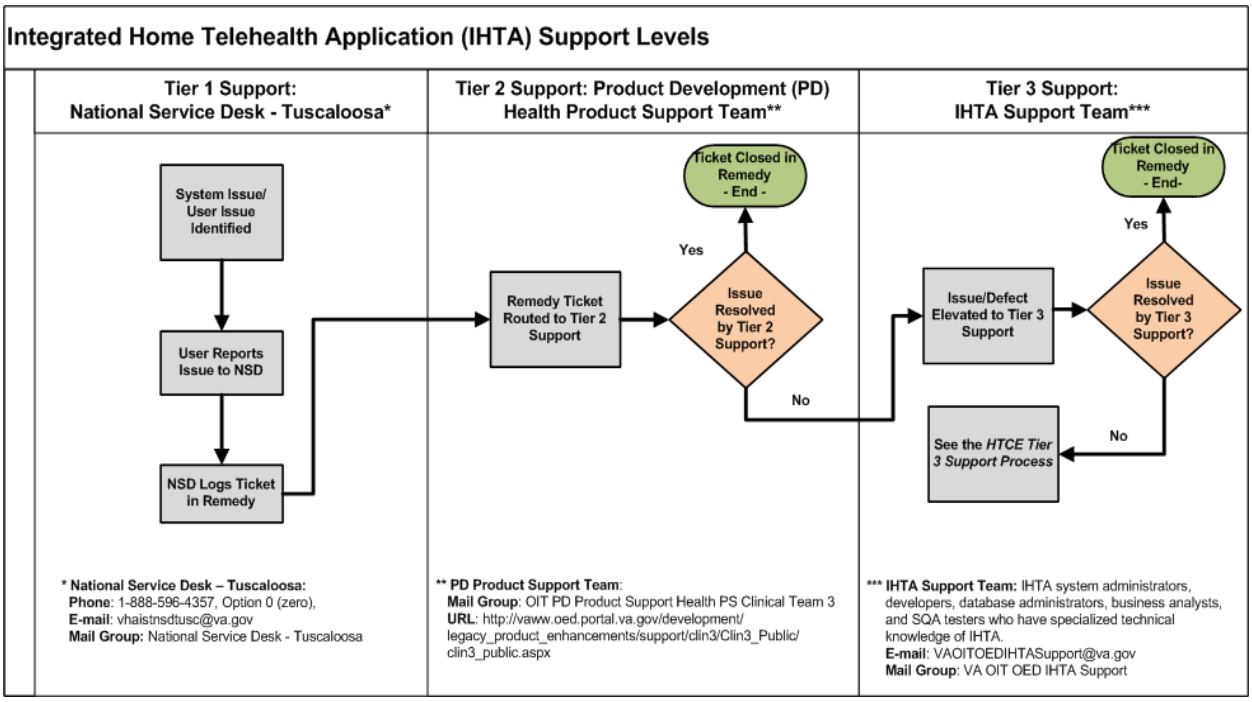

Figure 7: IHTA Support Levels: Tiers 1, 2 & 3

Tier 2 Support will assign Remedy Tickets to Tier III Production Support (IHTA Support Team) when an issue arises they cannot resolve (refer to Figure 7).

5 Contingency Planning

5.1 Continuity of Operations

This section describes the failover procedure that the IHTA and HT support staff will execute in order to maintain an available system and to mitigate the impact of any unscheduled or scheduled downtime. The procedures described in this section refer to the process of switching normal system operations from Martinsburg to Hines and back.

5.1.1 Switchover from Martinsburg to Hines

The following steps outline the failover procedure from the Primary Facility to the Secondary Facility:

1. Shutdown the WebLogic cluster at Martinsburg.
    a. Log onto **vhacrbappihta91.HTRE.cc.med.va.gov.**
    b. At the Linux command line, run the following commands
        i. **sudo su - wlp_user**
        ii. **stopenv.sh prod.properties <node manager port number>**
2. Contact the HT DBA to switch the primary HT Production Database from Martinsburg to Hines.

Database Tasks

a. Coordinate with other application users of HT and the DBAs informing them that the mirror switch-over is going to occur.
b. Using the MS SQL Server Management Studio tool, identify the 'principal' database to be switched. The 'principal' database is the primary database of a mirrored pair.
c. Identify the secondary database that will become the primary database after the switch. The secondary is part of the mirrored pair, usually found on a separate server. The database name will be the same but the database will be in a 'synchronized/restoring' state.
d. Right clicking on the primary database name select **tasks** > **mirror**.
e. Select 'failover' and agree to continue.
f. The database server will place the primary database in the 'synchronized/restoring' state and the secondary database in the 'principal' state. The secondary database becomes the 'new primary' and will be referred to as such in the remaining portions of these instructions.
g. The new primary database will have the miss configured user metadata so scripts will need to be run to make corrections.
h. In the new primary database, access and run the **bld_temp_schema_owner.sql** script from the SQL script library. This script creates a local user in the new primary database and gives them ownership of any schemas that are owned by the HTRE application users whose metadata and ability to sign on to the database has become compromised.
i. Run the script **rebld_htie_users.sql**. This script re-creates the connection between the HTRE application database user and the HTRE database login the user should be associated with. Users that own the application schemas are returned to that ownership.
j. Run the script **rebld_wl_login.sql.** This script reestablishes the WebLogic database ownership to the user WEBLOGIC.
k. Send notification that the database has been flipped.

3. Start the WebLogic cluster at Hines.
    a. Log onto **vhaishappihta81.vha.med.va.gov**
    b. At the Linux command line, run the following commands:
        i. **sudo su - wlp_user**;
        ii. **startnodemanager.sh <node manager port>**
        iii. **startenv.sh prod.properties**
4. Contact the HT Load Balancer Administrator to configure the HT Load Balancer to direct network traffic to Hines.

5.1.2 Switchover from Hines to Martinsburg

The following steps outline the failover procedure from Hines to Martinsburg:

1. Shutdown the WebLogic cluster at Hines.
    a. Log onto **vhaishappihta81.vha.med.va.gov.**
    b. At the Linux command line, run the following commands:
        i. **sudo su - wlp_user**
        ii. **stopenv.sh prod.properties <node manager port number>**

2. Contact the HT DBA to switch the primary HT Production Database from Hines to Martinsburg.

   Database Tasks

   a. Coordinate with other application users of HT and DBAs informing them that that the mirror switch-over is going to occur.
   b. Use SQL Server Management Studio (SSMS), flip the mirroring sites.
   c. Use the SSMS run script **'build_temp_schema_owner.sql**' to transfer schema ownership to temporary user.
   d. Use SSMS run script '**rebuild_htie_login_user.sql**' to rebuild IHTA users and reclaim schema ownership.
   e. Use SSMS run script '**rebuild_weblogic_login_user.sql**' to rebuild the WebLogic login database ownership.
   f. Validate the user changes.
   g. Send a notification that the database has been flipped.
3. Manually adjust the HTRE/IHTA and WebLogic user IDs at Martinsburg to enable access to the database objects that they have permission to access.
4. Start the WebLogic cluster at Martinsburg.
   a. Log onto **vhacrbappihta91.HTRE.cc.med.va.gov.**
   b. At the Linux command line, run the following commands:
      i. **sudo su - wlp_user**
      ii. **startnodemanager.sh <node manager port>**
      iii. **startenv.sh prod.properties**
5. Contact the HT Load Balancer Administrator to configure the HT Load Balancer to direct network traffic to Martinsburg.

5.1.3 Contingency Plan Contact Information

This section lists the names, phone numbers, and e-mail addresses of the leaders who must be notified in an emergency situation. This notification list will be checked for accuracy every month.

IHTA POCs:

Role	Name	Phone	E-Mail
Primary POC	David Komraus	(248) 737-2967	david.komraus@va.gov
Secondary POC	Chuck Lee	(502) 226-0557	charlesr.lee@va.gov

Facility POCs:

Role	Name	Phone	E-Mail
Primary POC	George Bracy	(708) 786-5895	george.bracy2@va.gov
Secondary POC	Dave Lindgren	(708) 786-5849	dave.lindgren@va.gov

Contact Information Last Reviewed and Updated on:	**04/10/2014**

5.1.4 Emergency Procedures

Refer to the SOPs, DRPs, and Contingency Plans at the Primary and Secondary Facilities for the standard emergency procedures in effect.

5.1.5 Team Staffing and Tasks

Contingency Planning / Disaster Management (CP/DM) Team

Role	Name
Contingency Plan Coordinator (Team Leader)	David Komraus
Facilities Representative (To coordinate closely with Facility Engineer)	Chuck Lee
Technical Representative(s)	Chris Woodyard

Primary/Secondary Facility Team

Role	Name
Facility POC	George Bracy
Facility POC	Dave Lindgren

CP/DM Team

The CP/DM Team is responsible for providing overall direction of the data center recovery operations. It ascertains the extent of the damage, activates the recovery organization, and notifies the team leaders. Its prime role is to monitor and direct the recovery effort. It has a dual structure in that its members include Team Leaders of other teams.

The CP/DM Team Leader is responsible for deciding whether or not the situation warrants the introduction of DR procedures. If he/she decides that it does, then the organization defined in this section comes into force and, for the duration of the disaster, supersedes any current management structures.

The CP/DM Team is also responsible for restoring computer processing and for performing computer room activities.

The CP/DM Team will operate from a Virtual Command Center.

CP/DM Team Responsibilities

The CP/DM Team's responsibilities include the following:

- Making decisions about restoring the computer processing environment in order to provide the identified level of operational service to users.
- Managing all the recovery teams and liaising with the data centers, customers, and users, as appropriate.
- Maintaining audit and security control during the recovery from disaster.
- Controlling and recording emergency costs and expenditure.
- Ensuring that the standby equipment meets the recovery schedules.
- Obtaining all appropriate historical/current data from the vault location and restoring an up-to-date application systems environment.
- Providing the appropriate management and staffing of the standby computer processing center, data control, help desk and media control/tape library in order to meet the defined level of user requirements.

- Supporting operable versions of all critical applications needed to satisfy the minimum operating requirements.
- Performing backup activities at the Secondary Facility.
- Evaluating the extent of the problem and potential consequences.
- Notifying senior management of the disaster, recovery progress, and problems.
- Initiating DR procedures.
- Co coordinating and documenting recovery operations
- Monitoring recovery operations and ensuring that the schedule is met.
- Liaising with user management.
- Expediting authorization of expenditures by other teams if required.
- Making a detailed accounting of the damage to aid in insurance claims, if required.
- Ensuring that the conversion to the Secondary Facility and the final resumption of operations at the Secondary Facility are under sufficient audit control to provide reliability and consistency to the accounting records.
- Monitoring computer security standards.
- Ensuring that appropriate arrangements are made to restore the site and return to the status quo within the time limits allowed for emergency mode processing.
- Approving the results of audit tests on the applications which are processed at the Secondary Facility shortly after they have been produced.
- Performing a detailed audit review of the critical accounting files after the first back up cycle has been completed.
- Declaring that the DRP is no longer in effect when computer processing is restored at the Primary Facility.
- Providing ongoing technical support at the Secondary Facility.
- Restore local and wide area data communications services to meet the minimum processing requirements.
- Obtaining all necessary back-ups from off-site storage.
- Initiating operations at the Secondary Facility.
- Reestablishing software libraries and databases to the last backup.
- Co-coordinating the user groups to aid the recovery of any non-recoverable data
- Providing sufficient personnel to support operations at the Secondary Facility
- Reestablishing the Data Control and Media Control/Tape Library functions at the Secondary Facility.
- Establishing processing schedule and inform user contacts.
- Arranging for acquisition and/or availability of necessary computer supplies.
- Ensuring that all documentation for standards, operations, vital records maintenance, application programs, etc. are stored in a secure/safe environment and reassembled at the Secondary Facility, as appropriate.
- Informing employees of the recovery progress of the schedules.
- Informing customers of any potential delays; any other public relations.

Primary Facility Team

The Primary Facility Team is comprised of POCs at Martinsburg CRRC or HITC, depending on which facility is the current IHTA Primary site.

The Primary Facility Team is responsible for the general environment including buildings, services, and all environmental issues related to the primary server at Martinsburg CRRC.

NOTE: The Primary Facility has appropriate SOPs, DRPs, and Contingency Plans in place for each site. This plan will be used in conjunction with the SOPs of the appropriate data center to provide comprehensive operations recovery for IHTA.

Primary Facility Team's Responsibilities

The Primary Facility Team is responsible for the general environment including buildings, services, and all environmental issues related to the computer room housing the IHTA Production Servers.

- Administering the reconstruction of the original site for recovery and operation.
- Arranging all transport to the Secondary Facility.
- Controlling security at the Primary Facility and the damaged site.
- In conjunction with the DM Team, evaluating the damage and identifying equipment that can be salvaged.
- Working with the DM Team to have lines ready for rapid activation.
- As soon as the Secondary site is occupied, cleaning up the disaster site, and securing that site to prevent further damage.
- Arranging new local and wide area data communications facilities and a communications network, which links the Primary Facility to the critical users.
- Supplying information for initiating insurance claims.
- Evaluate the extent of damage to the voice and data network and discuss alternate communications arrangements with telecom service providers.
- Establish the network at the Primary Facility in order to bring up the required operations. Define the priorities for restoring the network in the user areas.
- Order the voice/data communications and equipment as required.
- Supervise the line and equipment installation for the new network.
- Providing necessary network documentation.
- Providing ongoing support of the networks at the Primary Facility.
- Re-establish the networks at the Primary Facility when the post disaster restoration is complete.
- Ensuring that insurance arrangements are appropriate for the prevailing circumstances (e.g., any replacement equipment is immediately covered, etc.).
- Installing a minimum voice network to enable identified critical telephone users to link to the public network.
- Preparing the original data center for re occupation.
- Maintaining current configuration schematics of the data center (stored off site). This should include: air conditioning, power distribution, electrical supplies and connections, and specifications and floor layouts.
- Controlling security within the disaster area.
- Arranging for all necessary office support services.
- Dealing with staff safety and welfare.

Secondary Facility Team

The Secondary Facility Team is comprised of POCs at Martinsburg CRRC or HITC, depending on which facility is the current IHTA Secondary site.

The Secondary Facility's Team is responsible for the general environment, including buildings, services, and all environmental issues related to the computer room housing the IHTA Backup Servers.

NOTE: The Secondary Facility has appropriate SOPs, DRPs, and Contingency Plans in place. This plan will be used in conjunction with the SOPs, DRPs, and Contingency Plan at the Secondary Facility to provide comprehensive operations recovery for IHTA.

Secondary Facility Team's Responsibilities

- The Secondary Facility's responsibilities include, but are not limited to, the following:
- Maintaining the IHTA DR equipment in a ready state.
- Working with the DM Team and the Primary Facility Team to transfer IHTA operations to the Secondary Facility (when required) as soon as possible after the disaster.
- Working with the DM Team and the Primary Facility Team to transfer IHTA operations back to the Primary Facility when the Primary Facility is operational once again.

5.1.6 Alternate Site Procedures

IHTA contingency/ disaster recovery planning will be managed at a Virtual Primary Command Center using a dedicated VANTS line and Microsoft Lync. This VANTS line will be available 24x7. A second VANTS line will be available on Secondary and will serve as the Alternative Site in the event that the first VANTS line is down.

5.1.7 Documentation List

The following list is a comprehensive list of all documentation pertinent to the operation and maintenance of IHTA:

- *HTRE Contingency Plan*
- *Home Telehealth Operations &Maintenance Plan*
- *HTRE Operations &Maintenance Plan*
- *HTRE Disaster Recovery Plan*
- *IHTA Production Operations Manual*
- Home Telehealth System Security Plans (vendor specific)*
- Home Telehealth Contingency Plans (vendor specific)*
- *HTRE Software Architecture Document*
- *HTRE Database Design Document*
- *Home Telehealth Contingency Plan* for vendor-related contingency planning
- SOPs, DRPs, and Contingency Plans at the Martinsburg CRRC and HITC
- Program-specific Service Level Agreement For Information Technology Services Agreement Between The Veterans Health Administration, Care Coordination Services/Care Coordination Home Telehealth and The Office of Information and Technology – June 2009

* The Home Telehealth Contingency Plans and Sensitive Security Plans (SSP) contain both system sensitive and vendor specific proprietary information. The six HT vendors are required to maintain and update the contingency plans and SSPs based on any system or personnel changes. The plans are housed on a restricted SharePoint with access on a need-to-know basis.

5.1.8 Inventory

This appendix lists the current software for the IHTA production environment.

Item / Vendor	Period of Performance	Contract Type
Microsoft SQL Server	2010-15	VA Enterprise License
Oracle Web Logic Portal Server	2010-15	VA Enterprise License
Apache Web Server	2010-15	Open Source

5.1.9 Hardware Inventory

The computer hardware for the production and back-up servers at both the Primary and Secondary Facilities are listed in the below table.

Mainframes/Processors/Servers		
Manufacturer	**Model, Description, Serial Number**	**Qty**
Martinsburg CRRC		
Dell	PowerEdge R510 Application Servers: Serial Numbers: HFS6VQ1, 1GS6VQ1 Web Servers: Serial Numbers: KT6VQ1, FKT6VQ1	4
Hines		
Dell	PowerEdge R510 Application Servers: Serial Numbers: CKT6VQ1,DKT6VQ1 Web Servers: Serial Numbers: BKT6VQ1,9KT6VQ1	4

5.1.10 Communications Requirements

Refer to the SOPs, DRPs, and Contingency Plans at the Primary and Secondary Facilities for communication requirements.

5.1.11 Vendor Contact Lists

This section is not applicable to IHTA, as the application (as of Release 6.5) does not need to work directly with Home Telehealth Vendors for any of the data/functionality.

5.1.12 External Support Agreements

Refer to the SOPs, DRPs, and Contingency Plans at the Primary and Secondary Facilities for external support agreements in effect.

5.1.13 Data Center/Computer Room Emergency Procedures and Requirements

Refer to the SOPs, DRPs, and Contingency Plans at the Primary and Secondary Facilities for the standard emergency procedures in effect.

5.1.14 Plan Maintenance Procedures

The plan maintenance procedures within this manual will initially be reviewed every six month (each PMAS released) and then annually by the HTRE-IHTA SA and DBA.

5.1.15 Contingency Log

A contingency log will be added to this appendix following the assessment and result of any exercise or real contingency operations. This log will be include a comprehensive lessons learned documenting unanticipated difficulties, staff participation, restoration of system backups, permanent lost data and equipment, and shut down of temporary equipment used for the resumption, recovery, and restoration.

5.2 Disaster Recovery

This plan has been designed and written to be used in the event of a disaster affecting the HTRE project's IHTA. IHTA is deployed to Production at the Martinsburg Capitol Region Readiness Center (CRRC) and the Hines Information Technology Center (HITC). At any given time, one of these sites will be the Primary IHTA Production site, and one will be the Secondary site. On a periodic basis, the Primary and Secondary sites will be switched, so that the current Primary site will become the Secondary site, and the current Secondary site will become the Primary site. Experience with other HT Information Technology (IT) systems has shown that this is the best way to ensure the Secondary site is fully capable of supporting IHTA operations in a Disaster Recovery scenario. IHTA is designed with redundant servers and services in order to provide one level of fault tolerance within the data center. Failures within the data center, such as the loss of a hard drive, power supply, or a network interface card, are assumed to be covered by the Standard Operating Procedures (SOP) established by the data center's local operations staff.

5.2.1 Purpose and Scope of This Plan

This plan has been designed and written to be used in the event of a disaster affecting the Primary and Secondary facilities hosting IHTA:

Capital Region Readiness Center
(CRRC)
VA Martinsburg Medical Center
510 Butler Avenue
Martinsburg, WV 25401

Hines Information Technology Center
Hines OIFO Bldg. 37
1st Ave and Cermak Rd.
Hines, IL 60141-7008

This plan is structured around teams, with each team having a set of specific responsibilities.

The decision to initiate disaster recovery procedures will be taken by the Disaster Management (DM) team leader or his deputy after assessing the situation following a disaster or crisis.

If the DM team leader decides to initiate disaster recovery procedures, then all members of the recovery teams will follow the procedures contained in this plan until recovery is complete.

This plan contains all the information necessary to restore an operational service in the event of a serious disruption of computer services at the above sites.

5.2.2 Updating This Plan

This plan must be kept up to date. It is the responsibility of the IHTA SA to ensure that procedures are in place to keep this plan up to date. If, while using the plan, you find any information which is incorrect, missing, or if you have a problem in understanding any part of this plan please inform IHTA SA so that it may be corrected. It is important that everyone understands his or her role as described in this plan.

Updated versions of the plan are distributed to the authorized recipients, listed in the following table.

5.2.3 Distribution List

The IHTA SA is responsible for distributing this plan. Each plan holder, listed in the table below, receives two copies of this plan. One copy is to be kept at the place of work and the other copy at home or other safe, off-site location. These copies have an official copy number.

Each team leader must ensure that each team member has two copies of the plan.

Distribution List

Name	Copy Number
DM Team Leader	**1, 2**
Operations Team Leader	**3, 4**
Primary Facility Team Leader	**4, 5**
Secondary Facility Team Leader	**6, 7**
Offsite Copy 1	**8**
Offsite Copy 2	**9**

5.2.4 Site Information (Locations, Deployment Recipients)

A disaster is defined as an incident that results in the loss of computer processing at the Martinsburg CRRC in Martinsburg, WV or the HITC (whichever is serving as Primary as the time of the disaster), to the extent that relocation to a Secondary Facility must be considered. A disaster can result from a number of accidental, malicious or environmental events such as fire, flood, terrorist attack, human error, and software or hardware failures.

The primary objective of this DRP is to ensure the continued operation of identified business critical systems in the event of a disaster.

Specific goals of the plan are:

- To be operational at the Secondary Facility within twelve (12) hours of a standby invocation.
- To operate at the Secondary Facility for up to seven (7) days.
- To reinstate IHTA within the maximum working standby period.
- To minimize the disruption to IHTA.

5.2.5 Disaster Management Team

The DM team is responsible for providing overall direction of the data center recovery operations. It ascertains the extent of the damage, activates the recovery organization, and notifies the team leaders. Its prime role is to monitor and direct the recovery effort. It has a dual structure in that its members include team leaders of other teams.

The DM team leader is responsible for deciding whether or not the situation warrants the introduction of disaster recovery procedures. If it does, then the organization defined in this section comes into force and, for the duration of the disaster, supersedes any current management structures.

The DM team operates from the Virtual Command Center. The members of the DM team are listed in the following table:

Disaster Management Team

Name	Work Phone	Cell Phone	Pager/other contact info
Chuck Lee	(501) 226-0557		charlesr.lee@va.gov
David Komraus	(248) 737-2967		david.komraus@va.gov
Chris Woodyard	(352) 337-0881		chris.woodyard@va.gov

5.2.5.1 Disaster Management Team Charter

The DM team is responsible for the following:

- Making decisions about restoring the computer processing environment in order to provide the identified level of operational service to users
- Managing all the recovery teams and liaising with IHTA's management, company headquarters and users, as appropriate
- Maintaining audit and security control during the recovery from disaster
- Evaluating the extent of the problem and potential consequences
    - Notifying senior management of the disaster, recovery progress and problems.
    - Initiating disaster recovery procedures
    - Co-coordinating recovery operations
    - Monitoring recovery operations and ensuring that the schedule is met
    - Documenting recovery operations
    - Liaising with user management
    - Ensuring that the conversion to the secondary facility and the final resumption of operations at the data center are under sufficient audit control to provide reliability and consistency to the accounting records
    - Monitoring computer security standards
    - Ensuring that appropriate arrangements are made to restore the site and return to the status quo within the time limits allowed for emergency mode processing

- Approving the results of audit tests on the applications which are processed at the secondary facility shortly after they have been produced
- Performing a detailed audit review of the critical accounting files after the first back up cycle has been completed
- Declaring that the DRP is no longer in effect when computer processing is restored at the primary site

5.2.6 Operations Team

The Operations team is responsible for the computer environment (computer room and other vital computer locations) and for performing tasks within those environments. This team is responsible for restoring computer processing and for performing computer room activities.

Operations Team

Name	Work Phone	Cell Phone	Pager/other contact info
Rey Ruiz	(512) 326-6046		reyes.ruiz@va.gov
Rashaka Boykins	(512) 981-4751		rashaka.boykins@va.gov

5.2.6.1 Operations Team Charter

The Operations Team is responsible for the following:

- Ensuring that the standby equipment meets the recovery schedules
- Installing the computer hardware and setting up the latest version of the operating system at the Secondary facility, this may be done together with the Secondary Facility team
- Obtaining all appropriate historical/current data and restoring an up to date application systems environment
- Providing the appropriate management and staffing of the Secondary computer processing center, data control, help desk and media control/tape library in order to meet the defined level of user requirements
- Support operable versions of all critical applications needed to satisfy the minimum operating requirements
- Performing backup activities at the Secondary site
- Providing ongoing technical support at the Secondary facility
    - Obtaining all necessary backups from off-site storage
    - Initiating operations at the Secondary facility
    - Re-establishing software libraries and databases to the last backup
    - Co-coordinating the user groups to aid the recovery of any non-recoverable (i.e., not available on the latest dump) data
    - Providing sufficient personnel to support operations at the Secondary facility
    - Re-establishing the data control and media control/tape library functions at the Secondary facility
    - Establishing processing schedule and inform user contacts
    - Arranging for acquisition and/or availability of necessary computer supplies

5.2.7 Primary Facilities Team

The Primary Facilities (CRRC & HITC) team is responsible for the general environment including buildings, services and all environmental issues outside of the computer rooms.

This team has responsibility for security, health and safety and for replacement building facilities.

5.2.7.1 Facilities Team Charter

- Administering the reconstruction of the original site for recovery and operation
- Arranging all transport to the Secondary facility.
- Controlling security at the Secondary facility and the damaged site. (Note: physical security may need to be increased.)
- In conjunction with the DM team, evaluating the damage and identifying equipment that can be salvaged
    - As soon as the Secondary facility is occupied, cleaning up the disaster site and securing that site to prevent further damage
    - Supplying information for initiating insurance claims.
    - Ensuring that insurance arrangements are appropriate for the prevailing circumstances (e.g., any replacement equipment is immediately covered)
    - Preparing the original data center for reoccupation
    - Maintaining current configuration schematics of the data center (stored offsite), to include:
        - Air conditioning
        - Power distribution
        - Electrical supplies and connections
        - Specifications and floor layouts
    - Controlling security within the disaster area
    - Arranging for all necessary office support services
    - Dealing with staff safety and welfare.

5.2.8 Secondary Facilities Team

The Secondary Facility's Team is comprised of POCs at Martinsburg or HITC, depending on which site is designated the IHTA Secondary site at the time of team activation. This team is responsible for the general environment, including buildings, services, and all environmental issues related to the computer room housing the IHTA Backup Servers.

NOTE: The Secondary Facility has appropriate SOPs, DRPs, and Contingency Plans in place. This DRP will be used in conjunction with the SOPs, DRPs, and Contingency Plans at the Secondary Facility to provide comprehensive operations recovery for IHTA.

5.2.9 What To Do in the Event of a Disaster

The most critical and complex part of the management of resources is in the planning and organization of the required personnel during the invocation of the plan.

Personnel must be well-rehearsed, familiar with the DRP, and be sure of their assignments.

5.2.10 Standard Emergency Procedures

The first priority in a disaster situation is to ensure safe evacuation of all personnel.

In the event of a major physical disruption, standard emergency procedures must be followed. This means immediately:

- Activating the standard alarm procedures for that section of the building to ensure that Medical, Security and Safety departments and emergency authorities are correctly alerted
- If necessary, evacuating the premises following the evacuation procedures and assemble outside at the designated location, if it is safe to do so

5.2.11 The First Steps for the Recovery Teams

- The Facilities team assesses the nature and extent of the problem
- If it is safe to do so, the Operations team switches off all equipment in the computer room, including air conditioners
- Building Security alerts the DM team leader
- The Facilities Team gives an initial assessment to the DM team leader, who needs to know the extent of the damage to the buildings and equipment and the staff status. Also report what actions have been taken

5.2.12 The Next Steps

The DM team leader decides whether to activate the DRP, and which recovery scenario will be followed.

The recovery teams then follow the defined recovery activities and act within the responsibilities of each team, as defined in this DRP.

5.2.13 Recovery Scenarios

There are two forms of recovery: Local Recovery (LR) and Disaster Recovery (DR). LR occurs when IHTA and data center POCs decide that it would take less time to correct the problem at the Primary Facility than to "change over" to the Secondary Facility. DR occurs when IHTA and data center POCs decide that IHTA needs to be activated at the Secondary Facility. LR and DR procedures are documented in the following subsections.

NOTE: Both the Primary and Secondary Facilities have appropriate SOPs, DRPs, and Contingency Plans in place. This plan will be used in conjunction with the SOPs for the appropriate facility to provide comprehensive operations recovery for IHTA.

5.2.13.1 Scenario One: Local Recovery

In this scenario, only a part of the computer processing environment is out of action, but the communication lines and network are still up and running. The goal of the recovery process in this case is to resolve IHTA issues at the Primary Facility. LR will be executed when IHTA and the Primary Facility POCs determine it would take less time to correct the problem at the Primary Facility than to "change over" to the Secondary Facility. The **Local Recovery Action Plan** is as follows:

To resolve IHTA issues at the Primary Facility, the following action plan will be implemented:

1. IHTA SA repairs network, hardware, software, or database.
2. IHTA SA restores corrupted files.
3. Testing staff performs quick regression test to verify that IHTA has been restored.

5.2.13.2 Scenario Two: Disaster Recovery

In this scenario, the entire computer processing environment (or most of it) is out of action. Communication lines and the network are out of action. The goal of the recovery process in this scenario is to move all identified applications to the Secondary facility. This scenario requires a full recovery procedure, as documented in this DRP. The **Disaster Recovery Action Plan** is as follows:

To activate IHTA at the Secondary Facility, perform the following in conjunction with the Secondary Facility's POCs:

1. IHTA Load Balancer should automatically direct attended (UI) traffic to the Secondary Facility (which will display a system down message).
2. IHTA DBA verifies the integrity of the database replication log files.
3. IHTA DBA executes stored proc to update the "identity" of all tables in the Secondary Facility.
4. IHTA SA confirms the software version in the Secondary Facility is the same as the Primary Facility.
5. IHTA SA brings up WebLogic clusters.
6. Testing staff performs quick regression test to verify application viability.

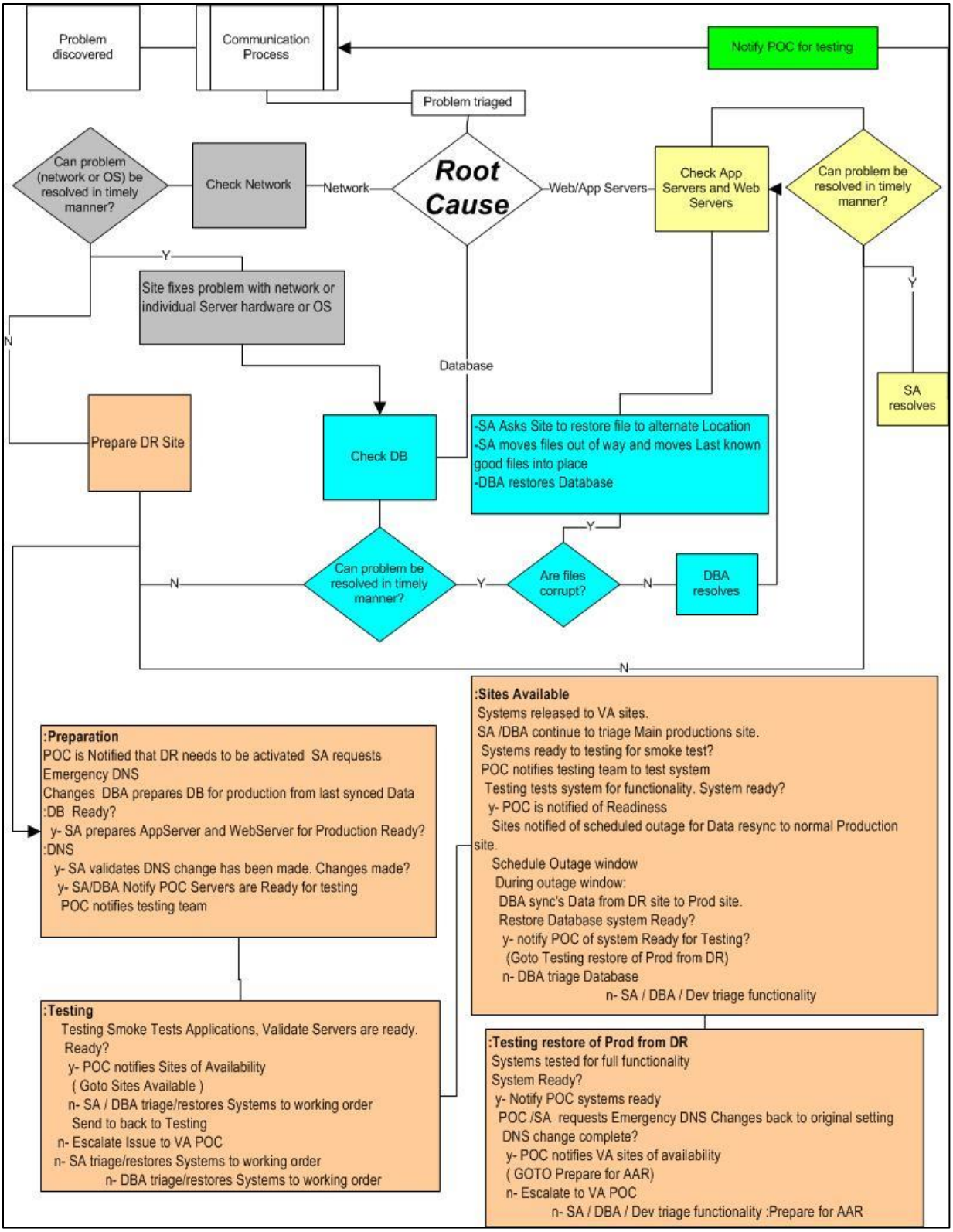

Figure 8: Flowchart of Local and Disaster Recovery Procedures

5.2.14 Recovery Activities

This section lists the activities key teams must perform to handle the disaster and restore IHTA operations at the Primary Facility.

5.2.15 Overview of the Tasks for Each Team

The following table provides an overview of the main responsibilities of each recovery team during the lifecycle of the disaster recovery process. The detailed tasks for each team are listed in the following sections.

Phase Team	Tasks During Normal Working Conditions on Site	Tasks Following Decision to Activate the Plan	Tasks While Plan is in Operation at Secondary Facility	Tasks After Return to the Primary Site
Disaster Management Team	Test the Plan	Evaluate damage	Make decisions	Make decisions
Disaster Management Team	Update the Plan	Ensure safety	Co-ordinate activities	Co-ordinate activities
Disaster Management Team	N/A	Call team meeting	Inform senior management	Inform senior management
Disaster Management Team	Test the Plan	Assess damage	Salvage operations	
Facilities Team	N/A	Attend team meeting	Security	Security
Facilities Team	N/A	N/A	Administration services	Administration services

Phase Team	Tasks During Normal Working Conditions on Site	Tasks Following Decision to Activate the Plan	Tasks While Plan is in Operation at Secondary Facility	Tasks After Return to the Primary Site
Facilities Team	N/A	Prepare/move to Secondary Facility	Supervise repairs and prepare for return to Primary Site	Supervise re-occupation of Primary Site or move to new permanent site
Operations Team	Test the Plan	Attend team meeting	Move to Secondary Facility	Reinstate computer processing
Operations Team	N/A	Prepare move to Secondary Facility	Operate the Secondary Facility	N/A

5.2.16 Immediate

1. Receive an initial assessment of the nature and extent of the problem.
2. Decide whether to activate the DRP.
3. Alert all Recovery Team Leaders (DM, Primary Facility, and Secondary Facility Team Leaders).
4. Alert and mobilize all other team members as required.
5. Make a preliminary (verbal) report to senior management.
6. Call an initial meeting of the Recovery Team Leaders with the following objectives:
    - To define the problem, the extent of the disruption, its consequences and the probable implications for the foreseeable future.
    - To set up a specified location as a Virtual Command Center (i.e., dedicated VANTS line).
    - To agree on each team's objectives for the next 3 (three) hours.
    - To set up a second meeting for 3 (three) hours later.
7. Make a second, more detailed, report to senior management on the content of the meeting and the actions being taken.

5.2.17 Within Three (3) Hours

8. Call a second meeting of the recovery team leaders with the following objectives:
    - To receive initial reports from the recovery team leaders.
    - To take the decision to implement disaster recovery procedures.
    - To agree each team's objectives for the next twenty-four (24) hours.
    - To set up a third meeting for twenty-four (24) hours later.
9. Contact all operations, data preparation, data control, and networks staff; inform all staff of the problem and the actions being taken
10. Ensure all staff remains calm and understand their roles.
11. Inform all staff of any temporary instructions.
12. Inform all user contacts of the nature and extent of the problem, telling them that they will be kept informed of the plans to recover.

5.2.18 Within Twenty-Four (24) Hours

13. Prepare plans for the transition to the Secondary Facility.
14. Make official declarations (e.g., place of work change to any regulatory authorities, etc.).
15. Report progress to senior management.
16. Contact suppliers of: hardware, communications equipment, and ancillary equipment.
17. Inform them of the arrangements for moving to the Secondary Facility.
18. Initiate 'interim' back up procedures for priority systems (this may involve manual procedures).
19. Brief all operations staff required to travel to the interim site(s) (if applicable).

20. Call all user contacts on a regular basis, advising them of the disruption and the actions being taken.
21. In conjunction with the Primary Facility, monitor the delivery and installation of new/replacement hardware, communications and ancillary equipment.
22. In the light of the disruption, review all production schedules in terms of jobs to be run, timings, priorities and dependencies.
23. Prepare production schedules in readiness for startup at the Secondary Facility.
24. Initialize and test the systems: hardware, operating systems, and communications network.
25. Before undertaking any processing, take security copies of all files and programs.
26. Transfer security copies to off-site storage location.
27. Start processing in accordance with prepared production schedules.
28. Discontinue work at any interim site(s).

5.2.19 Ongoing

29. Monitor, on a regular basis, all activities to exercise and maintain control over delivery and deployment dates.
30. Document progress against agreed schedules.
31. Monitor the network's performance.

5.3 Primary Facility Team's Tasks

The following subsections outline the Primary Facility team's tasks during a DR and or LR scenario. As stated, the Secondary Facility maintains its own SOPs, DRPs, and Contingency Plans; however, several of the primary tasks are outlined in the following subsections.

5.3.1 Immediate

1. Provide an initial damage report to the DM Team Leader.
2. Alert and mobilize all other team members.
3. Attend the initial meeting called for recovery team leaders.

5.3.2 Within Three (3) Hours

4. Conduct an asset inventory.
5. Make a full evaluation of the damage.
6. In conjunction with the DM Team, identify all potentially salvageable equipment.
7. Carry out safety inspections.
8. Make the site secure, to prevent unauthorized access by staff or the public.
9. Estimate the time required to recover.
10. Report back at the second meeting of recovery team leaders.
11. Help to compile an inventory of surviving communications equipment (voice/data) and that to be acquired.

12. Ensure that all relevant documentation is at hand or retrieved from the off-site storage facility, for the reinstatement of the network.
13. Ensure that all documentation/information is available to connect the voice, local, and wide area network to the Secondary Facility.
14. Liaise with the Secondary Facility and telecom service providers to monitor progress of communications reinstatement.

5.3.3 Within Twenty-Four (24) Hours

15. Provide the required facilities for the Virtual Command Center (refer to *The Command Center* section).
16. Arrange hotel or other temporary accommodation for staff.
17. Set up transport arrangements to/from all temporary locations.
18. Set up an Administration Support Desk to handle all queries.
19. Transfer staff to temporary locations.
20. Remove vital documents from disaster site.
21. Remove re-usable equipment from disaster site.
22. Define the priorities for restoring the network on a gradual basis in order to provide a minimum initial communications requirement for normal operations.
23. Liaise with suppliers of communications equipment to ensure prompt delivery, if required.
24. Ensure that the reinstated communications network is operable and tested.
25. Provide ongoing support for the communications network and carry out any re-configuration of the reinstated network that may be necessary.

5.3.4 Ongoing

26. Set up administrative support services, including, but not limited to, secretarial typing/word processing, telephones, telex/fax, mail internal/external, office equipment, and stationery.
27. Remove salvaged items from the disaster area.
28. Set up security procedures at the Primary Facility.
29. Contact suppliers of essential services (electricity, gas, water) and make any arrangements required as a result of the disruption.
30. Supervise delivery and installations at the Primary Facility.
31. If needed to be provided at the Primary Facility, monitor the installation of: electricity, heating/lighting, air conditioning, fire detection systems, access control systems, and telephones.
32. Provide office furniture, if required.
33. Transfer tapes, discs, documentation, etc. from off-site store to the Primary Facility.
34. Monitor and deal with users' requests in the light of the restricted network.
35. Prepare an inventory of all communications equipment requiring replacement in order for the original computer processing environment to be re-utilized.
36. Order replacement equipment as required.

5.4 Original Application Restoration

This is a two-step restoration. The first step establishes the viability of the data center and the second step takes the DR data and applies it to the Primary Facility.

To restore IHTA at the Primary Facility, perform the following in conjunction with the Primary Facility's POCs:

1. Data center staff triages/restores network connectivity.
2. IHTA SA triages/restores and starts the application servers, Web servers, and load balancers.
3. (If applicable) IHTA DBA triages/restores database without data from the Secondary Facility.
4. Testing staff brings up the environment and performs local tests.
5. If environment passes local testing, it is deemed "viable". Communication occurs with the Secondary Facility to bring the Secondary Facility down.
6. Testing staff brings both environments down.
7. IHTA DBA replicates Secondary Facility log files and activates the database engine at the Primary Facility.
8. IHTA DBA executes stored proc to update the "identity" of all tables in the Secondary Facility.
9. Testing staff brings up environment and performs local tests.
10. If environment passes local testing, it is deemed "restored".

5.4.1 Disaster Recovery Communication Process

This section describes the communication process between IHTA, the Primary Facility, the Secondary Facility, and the relevant VA sites from the onset of a DR to its resolution.

The IHTA DR communication process is as follows:

1. An IHTA emergency occurs at the Primary Facility or the Secondary Facility.
2. The IHTA SA, DBA, and other key staff quickly evaluate the problem and decide whether the emergency is a LR or DR scenario.
3. The Primary Facility or the Secondary Facility's POC immediately calls the IHTA POC and says that the DRP needs to be activated.
4. The IHTA POC immediately tells the IHTA team that the DRP has been activated and directs them to provide technical support to the DM Team.
5. The IHTA POC immediately e-mails IHTA National, VISN, and Facility Administrators and adds the following message to the e-mail's subject line: "IHTA Disaster Recovery Plan Activated." The e-mail summarizes the problem and contains information about how to "work around" the disaster.
6. The Primary and Secondary Facilities initiate recovery procedures. If a change to the Secondary Facility was required, once the servers are running at the Secondary Facility, the IHTA POC e-mails the VA sites and puts the following message in the subject line: "IHTA servers running at the Disaster Recovery site and application is ready for use."

7. After IHTA recovers to the Primary Facility, the IHTA POC e-mails the IHTA National, VISN, and Facility Administrators and adds the following message to the subject line: "IHTA Has Returned to Normal Operations. Disaster Recovery Deactivated." The e-mail may contain information about how the disaster was resolved.
8. One week after the DRP has been deactivated, the IHTA POC, in consultation with the IHTA team and the Primary and Secondary Facilities' POCs, writes an After-Action Review and posts it on the HTRE SharePoint site. The report is a "lessons learned" review that describes the disaster and its resolution and lists suggestions for process improvements.

5.4.2 The Command Center

This section describes the Virtual Command Center, from where the DM Team will direct DR operations.

5.4.2.1 Primary Command Center

IHTA DR will be managed at a Virtual Primary Command Center using a dedicated VANTS line. This VANTS line will be available 24x7 and will be utilized for all LR and DR scenarios.

5.4.2.2 Alternative Command Center

A second VANTS line will be available on standby and will serve as the Alternative Command Center in the event that the first VANTS line is down.

5.4.2.3 Command Center Requirements

The only requirement for the Virtual Command Center is a dedicated VANTs line. Microsoft Lync and/or NetMeeting will be utilized as conditions permit.

5.4.3 The Secondary Facility

This section provides a general introduction to the Secondary Facility, which IHTA will utilize for computer processing following a DR scenario.

5.4.3.1 Location of the Secondary Facility

If Martinsburg CRRC is the Secondary facility, the address of the Secondary facility is:

Capital Region Readiness Center (CRRC)
VA Martinsburg Medical Center
510 Butler Avenue
Martinsburg, WV 25401

If Hines is the Secondary facility, the address of the Secondary Facility is:

Hines Information Technology Center
Hines OIFO Bldg. 37
1st Ave and Cermak Rd.
Hines, IL 60141-7008

5.4.3.2 Secondary Alert Confirmation Sheet

The following form is used to confirm the invocation of to the Secondary Facility. It must be completed by the DM Team Leader and communicated to the Secondary Facility's POC.

Company Name:	
Address:	
Telephone Number:	
Disaster Alert Agreement Number:	
Designated Site:	
Nature of Disaster:	
Estimated Duration of Usage of the Secondary Facility:	
Date Usage to Start:	
Name:	
Signature:	
Date:	

5.4.4 The Data Storage Location(s)

Full and transactionlog backups of HT data are performed through Microsoft SQL server utilities into folders on the local RAID (Redundant Array of Inexpensive Disks) array (full backup). The backup file created by SQL Server is picked up nightly by an EMC/LEGATO (http://www.emc.com) backup agent installed on the server. Once the backup is collected by LEGATO it is dumped on to tape and stored off-site at Iron Mountain®, a data protection and recovery company with headquarters in Boston, MA (http://www.ironmountain.com). More details on the backup procedures are provided below.

HT systems implement backup procedures using the defined backup media and according to a defined frequency. The specific procedures are provided below:

- The vendor provides system backup hardware / software and the expendable supplies (e.g., cartridge tape) required to meet the following:
    - Database log and/or transaction files are backed up **every 1 hour**, in between the full database backups which are performed daily. The business requirement is that no more than one hour of operational data is lost due to a hardware failure of the primary systems.
    - The defined frequency of collecting server data including the database backups is a **weekly** full server backups and daily incrementals to a removalable cartridge tape. Data is defined as: elements of the system input by the VA patient end-users; VA Care Coordinators; and vendor systems administrators. Data is typically stored in the database.

- Full server system backups are performed **weekly**. Full systems include all necessary disk files required to return the systems to a fully operational status. This includes operating systems, configuration files, general utilities, application software, supporting files and scripts. The folder that contains the database data and transactional log backups are included in this backup.Incremental server backups are performed **daily**. Incremental backups include all files that have changed since the last full backup and aid in returning the server to a fully operational status as of the point of failure. This includes operating systems, configuration files, general utilities, application software, supporting files and scripts. The folder that contains the database data and transactional log backups are included in this backup.

-

- The vendor supplies AITC with documentation indicating the tape backup times, tape naming convention, and what to label/name the tapes (File Ids).

In an effort to protect HT systems from loss or damage, vendors systems managers must ensure that a reliable, periodic method of backing up information systems is followed. Specific requirements include:

- HT systems must be monitored to ensure that successful backups are taking place.
- Monthly review of the backup inventory should be performed between the vendor and AITC to ensure storage requirements are being meet.
- Backup procedures for AITC must be documented by the vendor and provide to AITC at the live test demonstration. The backup procedures should be demonstrated as part of the live test demonstration.

An inventory of backup media will be maintained by AITC. AITC will provide a secure off-site location for the storage of back-up media. Media will be stored for a minimum of two weeks. AITC will be responsible for the disposal of electronic backup media on which electronic backup data is stored.

Vendor systems include the following contingency requirements:

- Use of secondary storage such as RAID
- Implement redundancy such as, redundant components, servers, and infrastructure
- Implement fault-tolerant systems
- Implement failover equipment and strategies.

Refer to the Vendor-specific SSPs and Implementation Plans for more information on the contingency requirements.

5.4.5 Critical Business Lessons

This section describes the system requirements for IHTA's critical business applications in the Secondary Facility.

It is divided into two sections: Class 1 systems ("must-have") and Class 2 systems (important), with the timescales for these systems to support the business. No Class 2 Systems will be required for the IHTA production environment.

5.4.5.1 Class 1 Systems

Table 9 lists the Class 1 Systems ("must-have") utilized by the IHTA production environment.

Table 9: IHTA Class 1 System Requirements

Timescale	Application	System Requirements (Hardware, Software, Communications, Data, Documentation) Number of Users
Within 24 hours of declaration of disaster	IHTA	Hardware: 2 Application servers; 2 Web servers (Production Only) Database servers: 1 Software: Oracle WebLogic and SQL Server Communications: Standard LAN connection for all HTRE servers Number of Users: 50 concurrent Documentation: Server manuals; Production Operations Manual, SOPs at Secondary Facility

5.4.5.2 Class 2 Systems

No Class 2 Systems (important) will be required for the IHTA production environment.

5.4.6 Supplies for the Secondary Facility

This section contains checklists of all supplies, documentation and equipment needed for the Secondary facility.

5.4.6.1 Supplies

Please refer to the SOPs, DRPs, and Contingency Plans at the Secondary Facility for the supplies that are needed.

5.4.6.2 Documentation

The systems documentation required is as follows.

Systems Documentation

Item	Location/Vendor	Comments
System Specifications	N/A	N/A
Program Specifications	N/A	N/A
File Specifications	N/A	N/A
Record Specifications	N/A	N/A
Support Manuals	Dell	Server manuals

The operations documentation required is as follows.

Operations Documentation

Item	Location/Vendor	Comments
Operations Standards And Procedures	N/A	N/A
Operations Manuals	http://tspr.vista.med.va.gov/warboard/anotebk.asp?proj=1219	N/A
Run Instructions	N/A	N/A
Job Control Sheets	N/A	N/A
Sample Input Documents	N/A	N/A
Network Documentation	N/A	N/A

5.4.6.3 Other Equipment

No other equipment is required for IHTA.

5.4.7 Directories

This section of the plan contains a series of directories. These directories contain the type of information which is most likely to change such as names, addresses, telephone numbers etc.

It is important to keep these directories up to date.

5.4.8 Emergency Services

Refer to the SOPs, the DRPs, and the Contingency Plans at both the Primary and Secondary Facilities for more information on directories.

5.4.9 Recovery Team Members

The IHTA Recovery Team is comprised of three teams – the DM Team, the Operations Management Team, and the Primary and Secondary Facility Team.

The staffing of these Recovery teams is listed in this section. The team leader is the first name in the list.

5.4.9.1 Disaster Management Team: Members and Contacts

Disaster Management Team

Name	Work Phone	Cell Phone	Pager/other contact info
Chuck Lee	(501) 226-0557		charlesr.lee@va.gov
David Komraus	(248) 737-2967		david.komraus@va.gov
Chris Woodyard	(352) 337-0881		chris.woodyard@va.gov

5.4.9.2 Operations Team: Members and Contacts

Operations Management Team

Name	Work Phone	Cell Phone	Pager/other contact info
Rey Ruiz	(512) 326-6046		reyes.ruiz@va.gov
Rashaka Boykins	(512) 981-4751		rashaka.boykins@va.gov

5.4.9.3 Networks Team: Members and Contacts

This section is not applicable to IHTA.

5.4.9.4 Facilities Team: Members and Contacts

Facilities Team

Name	Work Phone	Cell Phone	Pager/other contact info
George Bracy	(708) 786-5895		george.bracy2@va.gov
Dave Lindgren	(708) 786-5849		dave.lindgren@va.gov

5.4.9.5 Communications Team: Members and Contacts

This section is not applicable to IHTA.

5.4.9.6 First Aiders

Refer to the SOPs, DRPs, and Contingency Plans at both the Primary and Secondary Facilities for more information on first aid.

5.4.9.7 User Groups and Application Support

The below table lists the users who will provide support for IHTA.

Application Support Personnel

System/Application	Contact	Phone
IHTA	Chuck Lee	(502) 226-0557
HT Database	Chris Woodyard	(352) 337-0881

5.4.9.8 Vendor and Supplier Contacts

Refer to the *Home Telehealth Production Operations Manual* for vendor-related DR following an emergency.

5.4.10 Inventories

This section contains inventories of all computer hardware, software, and other equipment.

5.4.10.1 Computer Hardware

Computer Hardware

Manufacturer	Model, Description, Number Mainframes/Processors/Servers/Serial Number	Qty
Martinsburg CRRC		
Dell	PowerEdge R510 Application Servers: Serial Numbers: HFS6VQ1, 1GS6VQ1 Web Servers: Serial Numbers: KT6VQ1, FKT6VQ1	4
HITC		
Dell	PowerEdge R510 Application Servers: Serial Numbers: CKT6VQ1,DKT6VQ1 Web Servers: Serial Numbers: BKT6VQ1,9KT6VQ1	4

5.4.10.2 Noncomputer Equipment

This section is not applicable to IHTA.

5.4.10.3 Software Inventory

Software Inventory

Supplier	Name, Version, etc.	Qty	License No.
Microsoft	Microsoft SQL Server 2008		
Oracle	Oracle WebLogic Server 11*g* Release 1 (10.3.5)		
Apache	Apache HTTP Server Version 2.2.3		
Red Hat	Red Hat Enterprise Linux (RHEL) 510		

5.4.10.4 Operating Systems

This section is not applicable to IHTA.

5.4.10.5 Related Documentation

This section contains references to other key documentation, which must be copied and kept in the vault location, together with copies of this POM. This section contains references to other key documentation related to this DRP:

- *HTRE Database Design Document* for*:*
  - Data backup procedures
  - Type(s) of backups
  - Means of identification
  - Length of time that backups are kept
  - Frequency of backups
  - Times when backups are performed
  - Method of rotating sets of backups

- *Home Telehealth Production Operations Manual (POM)* for vendor-related DR
- Martinsburg CRRC and HITC SOPs, DRPs, and Contingency Plans

Appendix A – IHTA Installation Guide

IHTA_Installation_Guide.docx

In the PDF file of the POM, please click on the Attachments icon in the PDF file to view and open the IHTA Installation Guide.

6 Approval Signatures

From: Hans, Ellen A

Sent: Friday, February 27, 2015 1:02 PM

To: Hula, Catherine (HP)

Subject:Yes: Signatures needed for HTRE Production Operations Manual

Signed: _____ _____

Ellen Hans, VA Program Manager/IPT Chair Date

Signed:

From:Komraus, David (HP)

Sent: September 03, 2015 4:24 PM

To:

Hula, Catherine (HP)

Subject:

Yes: Signatures needed for HTRE Project Management Plan

_____ _____

David Komraus, HTRE Project Manager Date

Signed: _____ _____

Kevin Joyner, Business Sponsor Date